# Defense Logistics Agency

# Information Technology Standards


## Version 1.0
## April 2000

# Table of Contents


1. INTRODUCTION ..... 1

2. SYSTEMS MANAGEMENT ..... 2

2.1 Data Communications ..... 2

2.2 Telecommunications ..... 3

3. COMMUNICATIONS ..... 4

3.1 Network Standards ..... 4
3.1.1 Transmission Control Protocol ..... 4
3.1.2 User Datagram Protocol ..... 4
3.1.3 Internet Protocol ..... 4
3.1.4 Open-Systems Interconnection Transport Over IP-based Networks ..... 5

3.2 Network Application Support Services ..... 5
3.2.1 Electronic Mail ..... 5
3.2.2 Directory Services ..... 6
3.2.2.1 X.500 Directory Services ..... 6
3.2.2.2 Lightweight Directory Access Protocol ..... 6
3.2.2.3 Domain Name System ..... 6
3.2.3 Remote Access ..... 7
3.2.4 Network Time Synchronization ..... 7
3.2.5 Bootstrap Protocol ..... 8
3.2.6 Configuration Information Transfer ..... 8
3.2.7 Web Services ..... 8
3.2.7.1 Hypertext Transfer Protocol ..... 8
3.2.7.2 Uniform Resource Locator ..... 8
3.2.7.3 Connectionless Data Transfer ..... 9

3.3 Internetworking (Router) Standards ..... 9
3.3.1 Interior Routers ..... 10
3.3.2 Exterior Routers ..... 10

3.4 Subnetworks ..... 10
3.4.1 Local Area Network Access ..... 10
3.4.2 Point-to-Point Standards ..... 11
3.4.3 Combat Net Radio Networking ..... 12
3.4.4 Integrated Services Digital Network ..... 12
3.4.5 Asynchronous-Transfer Mode ..... 13
3.4.6 Satellite Communications ..... 16
3.4.6.1 Super High Frequency Satellite Terminal Standards Earth Terminals ..... 16
3.4.6.2 Phase-Shift Keying Modems ..... 16
3.4.7 Personal Communications Services and Mobile Cellular ..... 16

3.5 Transmission Media – LANs/CANs ..... 17

4. PRESENTATION ..... 18
4.1 Web Server ..... 18
4.2 Character-Based Interfaces ..... 18
4.3 Graphical User Interfaces (GUI) ..... 18
4.4 Graphics Services ..... 19
5. DISTRIBUTED COMPUTING ..... 20
5.1 Remote-Procedure Computing ..... 20
5.2 Distributed-Object Computing ..... 20
5.3 Middleware ..... 21
5.4 Transaction Processing ..... 22
6. COLLABORATIVE SERVICES ..... 23
6.1 Video Teleconferencing ..... 23
6.2 Workflow ..... 25
7. DATA MANAGEMENT ..... 26
7.1 Metadata ..... 26
7.2 Database ..... 26
8. SECURITY SERVICES ..... 27
8.1 Application Environment ..... 27
8.2 Auditing and Alarm Reporting ..... 28
8.3 Authentication ..... 28
8.4 Encryption and Transmission ..... 29
8.4.1 Security Algorithms ..... 29
8.4.2 Security Protocols ..... 30
8.4.3 Network Security ..... 30
8.4.4 Web Security ..... 31
8.5 Evaluation Criteria ..... 32
8.6 Public Key Infrastructure ..... 33
8.6.1 Certificate Profiles ..... 34
8.6.2 Operational Protocols and Exchange Formats ..... 34
8.6.3 Management Protocols ..... 34

8.6.4 Application Program Interfaces (APIs) ..... 35
8.6.5 Cryptography ..... 35

**9. APPLICATION MANAGEMENT ..... 36**

**9.1 Software Engineering ..... 36**

**9.2 Activity Model ..... 36**

**9.3 Data Model ..... 36**
9.3.1 Object Modeling ..... 37

**9.4 DoD Data Definitions ..... 37**

**10. INFORMATION EXCHANGE ..... 38**

**10.1 Data Interchange Services ..... 38**
10.1.1 Document ..... 38
10.1.2 Graphics Data ..... 40
10.1.3 Audio Data ..... 41
10.1.4 Video Data ..... 41
10.1.5 Product Data ..... 42
10.1.6 Storage Media ..... 43
10.1.6.1 Optical Storage Media ..... 43
10.1.6.2 Smart Cards ..... 43
10.1.6.3 Electronic Tags ..... 43

**10.2 Facsimile ..... 44**
10.2.1 Analog Facsimile Standards ..... 44
10.2.2 Digital Facsimile Standards ..... 44

**10.3 Electronic Data Interchange ..... 44**

**10.4 Global Positioning System ..... 45**

**11. OPERATING SYSTEM SERVICES ..... 46**

# 1. Introduction

Effective military operations must respond with a mix of forces, anywhere in the world, at a moment's notice. The ability for the information technology systems supporting these operations to interoperate—work together and exchange information—is critical to their success. The lessons learned from conflicts like Desert Shield/Desert Storm resulted in a new vision for the Department of Defense (DoD). Joint Vision 2010 (JV 2010) is the conceptual template for how America's Armed Forces will channel the vitality and innovation of their people, and leverage technological opportunities to achieve new levels of effectiveness in joint warfighting. The DoD JTA provides DoD systems with the basis for the needed seamless interoperability. The JTA defines the service areas, interfaces, and standards (JTA elements) applicable to all DoD systems, and its adoption is mandated for the management, development, and acquisition of new or improved systems throughout DoD.

DLA must interoperate with all of the DoD Services not only during wartime, but also during day-to-day operations to ensure the continued readiness of our forces. To ensure our ability to meet these requirements, DLA will adhere to the principle and spirit of the standards guidance provided in the DoD JTA. This document, DLA Information Technology Standards, identifies key technology service areas that relate directly to DLA mission operations, and provides guidance on standards associated with these areas. The standards and guidelines in this document are stable, technically mature, and commercially supported with implementations from multiple vendors. Standards and guidelines that do not yet meet these criteria, but are expected to mature to meet them in the near-term (within 3 years), are cited as "emerging standards" in the expectation that they will be mandated in future versions of the DoD JTA and the DLA Information Technology Standards document.

The DLA Information Technology Standards document is complementary to, and consistent with, the DoD JTA and other DoD programs and initiatives aimed at the development and acquisition of effective, interoperable information systems. These include DoD's Specification and Standards Reform; Implementation of the Information Technology Management Reform Act (ITMRA); Defense Modeling and Simulation Initiative; Evolution of the DoD TRM; Defense Information Infrastructure Common Operating Environment (DII COE); and Open Systems Initiative.

Development of the DLA Information Technology Standards is a collaborative effort, conducted by the Information Technology Architecture Team (ITAT), and directed and approved by the Information Technology Management Team (ITMT). Members represent all operational areas of DLA. The DLA Information Technology Standards document is a key element of the overall DLA Information Technology Architecture. Also included in the DLA IT Architecture are: the DLA IT Policy, which supports the Agency's strategic direction; the DLA Information Technology Solutions, which identifies appropriate hardware and software to support specific requirements; and the contracts which identify appropriate vehicles available to support the purchase of required items.

The DLA Information Technology Standards is a living document and will continue to evolve with the technologies, marketplace, and associated standards upon which it is based.

# 2. Systems Management

Network and Systems Management (NSM) provides the capability to manage designated networks, systems, and information services. This includes: controlling the network's topology; dynamically segmenting the network into multiple logical domains; maintaining network routing tables; monitoring the network load; and making routing adjustments to optimize throughput. NSM also provides the capability to review and publish addresses of network and system objects; monitor the status of objects; start, restart, reconfigure, or terminate network or system services; and detect loss of network or system objects in order to support automated fault recovery. A management system has four essential elements: management stations; management agents; management information bases (MIB); and management protocols, to which these standards apply.

## 2.1 Data Communications

Data communications management stations and management agents (in end-systems and networked elements) shall support the Simple Network Management Protocol (SNMP).

The following SNMP-related standard is mandated:

- IETF Standard 15/RFC-1157, Simple Network Management Protocol (SNMP), May 1990.

To standardize the management scope and view of end-systems and networks, the following standards are mandated for MIB modules of the management information base:

- IETF Standard 16/RFC-1155/RFC-1212, Structure of Management Information, May 1990.
- IETF Standard 17/RFC-1213, Management Information Base, March 1991.
- IETF RFC-1514, Host Resources MIB, September 1993.
- IETF Standard 50/RFC-1643, Definitions of Managed Objects for the Ethernet-like Interface Types, July 1994.
- IETF RFC-1757, Remote Network Monitoring Management Information Base, (RMON Version 1), February 1995.
- IETF RFC-1850, Open Shortest Path First (OSPF) Version 2 Management Information Base, November 1995.

*Emerging: Simple Network Management Protocol Version 3 (SNMPv3). The SNMPv3 Management Framework is described in IETF-Proposed Standard RFCs 2271-2275. SNMPv3 builds on the mandate SNMPV1 and addresses the deficiencies in SNMPv2 relating to security (e.g., authentication and privacy) and administration (e.g., naming of entities, usernames and key management, and proxy relationships). Implementations of the RFCs are undergoing interoperability tests as part of the process to advance these specifications from Proposed to Draft state.*

## 2.2 Telecommunications

Telecommunications management systems for telecommunications switches will implement the Telecommunications Management Network (TMN) framework.

To perform information exchange within a telecommunications network, the following TMN framework standards are mandated:

- ANSI T1.204, OAM&P – Lower Layer Protocols for TMN Interfaces Between Operations Systems and Network Elements, 1993.
- ANSI T1.208, OAM&P – Upper Layer Protocols for TMN Interfaces Between Operations Systems and Network Elements, 1993.
- ITU-T M.3207.1, TMN management service: maintenance aspects of B-ISDN management, 1996.
- ITU-T M.3211.1, TMN management service: Fault and performance management of the ISDN access, 1996.
- ITU-T M.3400, TMN Management Functions, 1992.
- ISO/IEC 9595 Information Technology – Open Systems Interconnection Common Management Information Services (CMIS), December 1991.
- ISO/IEC 9596-1:1998 Information Technology – Open Systems Interconnection – Common
- Management Information Protocol (CMIP) – Part 1: Specification.
- ISO/IEC 9596-2:1993 Information Technology – Open Systems Interconnection – Common
- Management Information Protocol (CMIP): Protocol Implementation Conformance Statement (PICS) proforma.

# 3. Communications

## 3.1 Network Standards

The transport services provide host-to-host communications capability for application support services. The following sections define the requirements for this service.

### 3.1.1 Transmission Control Protocol

Transmission Control Protocol (TCP) provides a reliable connection-oriented transport service.

The following standards are mandated:

- IETF Standard 7/RFC-793, Transmission Control Protocol, September 1981. In addition, PUSH flag and the NAGLE Algorithm, as defined in IETF Standard 3, Host Requirements, are mandated.
- IETF RFC-2001, TCP Slow Start, Congestion Avoidance, Fast Retransmit, and Fast Recovery Algorithms, January 1997.

### 3.1.2 User Datagram Protocol

User Datagram Protocol (UDP) provides an unacknowledged, connectionless datagram transport service.

The following standard is mandated:

- IETF Standard 6/RFC-768, User Datagram Protocol, 28 August 1980.

### 3.1.3 Internet Protocol

Internet Protocol (IP) is a basic connectionless datagram service. All protocols within the IP suite use the IP datagram as the basic data transport mechanism. Two other protocols are considered integral parts of IP: the Internet Control Message Protocol (ICMP) and the Internet Group Management Protocol (IGMP). ICMP is used to provide error reporting, flow control, and route redirection. IGMP provides multicast extensions for hosts to report their group membership to multicast routers.

The following standard is mandated:

- IETF Standard 5/RFC-791/RFC-950/RFC-919/RFC-922/RFC-792/RFC-1112, Internet Protocol, September 1981. In addition, all implementations of IP must pass the 8-bit Type-of-Service (TOS) byte transparently up and down through the transport layer as defined in IETF Standard 3, Host Requirements.

Furthermore, for hosts that transmit or receive multi-addressed datagrams over Combat Net Radio (CNR), the multi-addressed IP option field must be used.

The following standard is mandated:

- ETF Informational RFC 1770, IPv4 Option for Sender Directed Multi-Destination Delivery, 28 March 1995.

*Emerging: IP Next Generation/Version 6 (IPv6). IPv6 is being designed to provide better internetworking capabilities than are currently available within IP (Version 4). IPv6 will include support for the following: expanded addressing and routing capabilities, authentication and privacy, autoconfiguration, and increased quality of service capabilities. Refer to RFC 2460 for details.*

*Also emerging is the Mobile Host Protocol (MHP). This protocol allows the transparent routing of IP datagrams to mobile nodes in the Internet. Each mobile node is always identified by its home address, regardless of its current point of attachment to the Internet. A mobile IP protocol is currently available as an IETF-proposed standard, RFC 2002, entitled IP Mobility Support.*

### 3.1.4 Open-Systems Interconnection Transport Over IP-based Networks

This protocol provides the interworking between Transport Protocol Class 0 (TP0) and TCP transport service necessary for Open-Systems Interconnection (OSI) applications to operate over IP-based networks.

The following standard is mandated:

- IETF Standard 35/RFC 1006, ISO Transport Service on top of the TCP, May 1987.

## 3.2 Network Application Support Services

### 3.2.1 Electronic Mail

The standard for official organizational-messaging traffic between DoD organizations is the Defense Message System's (DMS) X.400-based suite of military messaging standards defined in Allied Communication Protocol (ACP) 123. The ACP 123 annexes contain standards profiles for the definition of the DMS "Business Class Messaging" (P772) capability and the Message Security Protocol (MSP). Organizational messaging is considered a high-assurance messaging service that requires authentication, delivery confirmation, and encryption. See Section 2.6 for security standards.

The following standards are mandated:

- ACP 123, Common Messaging Strategy and Procedures, November 1994.
- ACP 123, U.S. Supplement No. 1, Common Messaging Strategy and Procedures, November1995.

DMS has expanded its baseline to include a medium-assurance messaging service. The requirements for medium-assurance messaging are less stringent than organizational messaging and can be met by existing IP-based mail standards. This allows the augmentation of DMS to include the use of the Simple Mail Transfer Protocol (SMTP) for medium-assurance messaging.

For SMTP, the following standards are mandated:

- IETF Standard 10/RFC-821/RFC-1869/RFC-1870, Simple Mail Transfer Protocol (SMTP) Service Extensions, November 1995.
- IETF Standard 11/RFC-822/RFC-1049, Standard for the Format of ARPA Internet Text Messages, 13 August 1982.
- IETF RFCs 2045-2049, Multipurpose Internet Mail Extensions (MIME) Parts 1-5, November 1996.

## *3.2.2 Directory Services*

### 3.2.2.1 X.500 Directory Services

International Telecommunications Union (ITU) X.500 provides directory services that may be used by users or host applications to locate other users and resources on the network. While it is appropriate for all grades of service, it must be used for high-grade service where standards-based access control, signed operations, replication, paged results, and server-to-server communication are required. It provides the security services used by DMS-compliant X.400 implementations and is mandated for use with DMS. See Section 2.6 for security standards. See Section 5.1, Remote Procedure Computing, for directory services standards to be used in a remote-procedure computing environment.

The following standard is mandated:

- ITU-T X.500, The Directory – Overview of Concepts, Models, and Services – Data Communication Networks Directory, 1993.

### 3.2.2.2 Lightweight Directory Access Protocol

Lightweight Directory Access Protocol (LDAP) (Version 2) is an Internet protocol for accessing online directory services. It runs directly over Transmission Control Protocol (TCP). LDAP derives from the X.500 Directory Access Protocol (DAP). It is appropriate for systems that need to support a medium grade of service in which security is not an issue, and access is only needed to a centralized server.

The following standard is mandated:

- IETF RFC-1777, Lightweight Directory Access Protocol, March 1995.

*Emerging: Lightweight Directory Access Protocol 3 (LDAPv3). The proposed standard for LDAPv3, IETF RFC 2251, supports standards-based authentication, referrals, and all protocol elements of LDAP (IETF RFC 1777). Other features still under development include standards-based access control, signed operations, replication, knowledge references, and paged results.*

### 3.2.2.3 Domain Name System

Domain Name System (DNS) is a hierarchical host management system that has a distributed database. It provides the look-up service of translating between host names and IP addresses. DNS uses TCP/User Datagram Protocol (UDP) as a transport service when used in conjunction with other services.

The following standard is mandated:

- IETF Standard 13/RFC-1034/RFC-1035, Domain Name System, November 1987.

*Emerging: Dynamic Domain Name System. The Dynamic Domain Name System (DDNS) protocol defines extensions to the Domain Name System (DNS) to enable DNS servers to accept requests to update the DNS database dynamically. DDNS is referenced in RFC 2136.*

*The Domain Name System (DNS) has become a critical operational part of the Internet infrastructure, yet it has no strong security mechanisms to ensure data integrity or authentication. IETF RFC-2065, "DNS Security Extensions," D. Eastlake, C. Kaufman, January 1997, describes extensions to the DNS that provide these services to security-aware resolvers or applications through the use of cryptographic digital signatures. These digital signatures are included in secured zones as resource records. Security can still be provided even through non-security-aware DNS servers in many cases. The extensions also provide for the storage of authenticated public-keys in the DNS. This storage of keys can support general public-key distribution service as well as DNS security.*

### 3.2.3 Remote Access

Basic File Transfer is accomplished using the File Transfer Protocol, which provides a reliable file transfer service for text or binary file. FTP uses TCP as a transport service.

The following standard is mandated:

- IETF Standard 9/RFC-959, File Transfer Protocol, October 1985, with the following FTP commands mandated for reception: Store unique (STOU), Abort (ABOR), and Passive (PASV).

*Emerging: RFC-2228, File Transfer Protocol, October 1997, defines extensions to the FTP standard (STD9/RFC 959). These extensions provide strong authentication, integrity, and confidentiality on both the control and data channels. RFC-2228 also introduces new optional commands, replies, and file transfer encodings.*

For ASCII text-oriented remote-terminal services, Telecommunications Network (TELNET) provides a virtual terminal capability that allows a user to "log on" to a remote system as though the user's terminal were directly connected to the remote system.

The following standard is mandated:

- IETF Standard 8/RFC-854/RFC-855, TELNET Protocol, May 1983.

*Emerging: Secure Shell (SSH) is a protocol used to log into another computer over a network to execute commands in a remote machine, and to move files from one machine to another. It provides strong authentication and secure communications over insecure channels. Once this protocol is adopted, remote shell, remote login, and remote copy are not to be used.*

### 3.2.4 Network Time Synchronization

Network Time Protocol (NTP) provides the mechanisms to synchronize time and coordinate time distribution in a large, diverse internet.

The following standard is mandated:

- IETF RFC-1305, Network Time Protocol (Version 3) Specification, Implementation, and Analysis, March 1992.

### 3.2.5 Bootstrap Protocol

Bootstrap Protocol (BOOTP) is used to provide address determination and bootfile selection. It assigns an IP address to workstations with no IP address.

The following standards are mandated:

- IETF RFC-951, Bootstrap Protocol, September 1985.
- IETF RFC-2132, DHCP Options and BOOTP Vendor Extensions, March 1997.
- IETF RFC-1542, Clarifications and Extensions for the Bootstrap Protocol, October 1993.

### 3.2.6 Configuration Information Transfer

The Dynamic Host Configuration Protocol (DHCP) provides an extension of BOOTP to support the passing of configuration information to Internet hosts. DHCP consists of two parts: a protocol for delivering host-specific configuration parameters from a DHCP server to a host, and a mechanism for automatically allocating IP addresses to hosts.

The following standard is mandated:

- IETF RFC-2131, Dynamic Host Configuration Protocol, March 1997.

### 3.2.7 Web Services

#### 3.2.7.1 Hypertext Transfer Protocol

Hyptertext Transfer Protocol (HTTP) is used for search and retrieval within the Web. HTTP uses TCP as a transport service.

The following standard is mandated:

- IETF RFC-2616, Hypertext Transfer Protocol – HTTP/1.1, June 1999.

#### 3.2.7.2 Uniform Resource Locator

A Uniform Resource Locator (URL) specifies the location of, and access methods for, resources on the Internet.

The following standards are mandated:

- IETF RFC-1738, Uniform Resource Locators (URL), 20 December 1994.
- IETF RFC-1808, Relative Uniform Resource Locators, June 1995.

#### 3.2.7.3 Connectionless Data Transfer

The Connectionless Data Transfer Application Layer Standard allows Variable Message Format (VMF) messages to be used in connectionless applications. This standard uses TCP/UDP as a transport service.

The following standard is mandated:

- MIL-STD-2045-47001B, Connectionless Data Transfer Application Layer Standard,

## 3.3 Internetworking (Router) Standards

Routers are used to interconnect various subnetworks and end-systems. Protocols necessary to provide this service are specified below. RFC-1812 is an umbrella standard that references other documents and corrects errors in some of the referenced documents. In addition, some of the standards that were mandated for hosts in Section 3.1also apply to routers. Routers exchange connectivity information with other routers to determine network connectivity and adapt to changes in the network. This enables routers to determine, on a dynamic basis, where to send IP packets.

The following standards are mandated:

- IETF RFC-1812, Requirements for IP Version 4 Routers, 22 June 1995.
- IETF Standard 6/RFC-768, User Datagram Protocol, 28 August 1980.
- IETF Standard 7/RFC-793, Transmission Control Protocol, September 1981.
- IETF Standard 8/RFC-854/RFC-855, TELNET Protocol, May 1983.
- IETF Standard 13/RFC-1034/RFC-1035, Domain Name System, November 1987.
- IETF RFC-951, Bootstrap Protocol, September 1985.
- IETF RFC-2132, DHCP Options and BOOTP Vendor Extensions, March 1997.
- IETF RFC-2131, Dynamic Host Configuration Protocol, March 1997.
- IETF RFC-1542, Clarifications and Extensions for the Bootstrap Protocol, October 1993.
- IETF Standard 33/RFC-1350, The TFTP Protocol (Revision 2), July 1992, to be used for initialization only.

*Emerging: Quality of Service (QoS) is the ability of a network to ensure that the predetermined traffic and service requirements of a network element (e.g., end-system, router, application) can be satisfied. Multiple fora including the IETF and IEEE are engaged in this evolving end-to-end networking effort to enhance the current networking architecture with support for QoS. To provide services over the LAN/WAN beyond the current best-effort IP-based service, the protocols currently under development to enable end-to-end QoS includes the Resource Reservation Protocol (RSVP). RSVP communicates the QoS requirements for a given application to a device in the path of the transmission. A reservation for the required bandwidth is allowed or denied depending on the current network conditions. RSVP is expected to be utilized predominantly in the campus-level networks. RFC 2205, Resource ReSerVation Protocol (RSVP)—Version 1, RFC 2207 (RSVP Extensions for IPSEC), and RFC 2380 (RSVP over ATM) are all emerging standards.*

*Also emerging are IEEE 802.1p and IEEE 802.1Q. These IEEE standards specify the traffic classification method used by Ethernet switches, to expedite delivery of time critical traffic. IEEE 802.1p governs the prioritization of packets, offering eight discrete priority levels from the default (best effort) through reserved (highest priority). IEEE 802.1Q defines an additional 4-octet field in the LAN header to support Virtual LANs.*

### 3.3.1 Interior Routers

Routes within an autonomous system are considered local routes that are administered and advertised locally by means of an interior gateway protocol.

For unicast interior gateway routing, the following standard is mandated:

- IETF Standard 54/RFC-2328, Open Shortest Path First Routing Version 2, April 1998.

### 3.3.2 Exterior Routers

Exterior gateway protocols are used to specify routes between autonomous systems. For exterior gateway routing, Border Gateway Protocol 4 (BGP-4) uses TCP as a transport service.

The following standards are mandated:

- IETF RFC-1771, A Border Gateway Protocol 4 (BGP-4), 21 March 1995.
- IETF RFC-1772, Application of the Border Gateway Protocol in the Internet, March 1995.

## 3.4 Subnetworks

This section identifies the standards needed to access subnetworks used in joint environments.

### 3.4.1 Local Area Network Access

While no specific Local Area Network (LAN) technology is mandated, the following is required for interoperability in a joint environment. This requires provision for a LAN interconnection. Ethernet, the common implementation of Carrier Sense Multiple Access with Collision Detection (CSMA/CD), is the most common LAN technology in use with TCP/IP. The hosts use a CSMA/CD scheme to control access to the transmission medium. An extension to Ethernet, Fast Ethernet provides interoperable service at both 10 Mbps and 100 Mbps. Platforms that must physically connect to a joint task force local area network shall support the 10BASE-T connection for Ethernet. When a higher-speed interconnection is required, 100BASE-TX (two pairs of Category5 unshielded twisted pair) may be employed. The 100BASE-TX Auto-Negotiation features are required when 100BASE-TX is deployed to permit interoperation with 10BASE-T.

The following standards are mandated as the minimum LAN requirements for operation in a joint task force:

- ISO/IEC 8802-3:1996, Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications, 10BASE-T Medium-Access Unit (MAU).

- IEEE 802.3u-1995, Supplement to ISO/IEC 8802-3:1993, Local and Metropolitan Area Networks: Media Access Control (MAC) Parameters, Physical Layer, Medium Attachment Units, and Repeater for 100 Mbps Operation, Type 100BASE-T (Clauses 21-30).
- IETF Standard 41/RFC-894, Standard for the Transmission of IP Datagrams Over Ethernet Networks, April 1984.
- IETF Standard 37/RFC-826, An Ethernet Address Resolution Protocol, November 1982.

*Emerging: Wireless LAN. The IEEE 802.11 Wireless LAN protocol was finalized in June 1997 as IEEE 802.11-1997 Part II: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. It provides a common set of operational rules for airwave interoperability of wireless LAN products from different vendors. It specifies both direct-sequence spread-spectrum and frequency-hopping spread-spectrum physical layers for wireless radio-based LANs. Also, it includes infrared connectivity technologies. An Inter Access Point protocol is being developed to provide a standardized method for communications between wireless LAN access points.*

*Also emerging is Gigabit Ethernet. Gigabit Ethernet provides service at 1,000 Mbps. For physical layer and framing requirements, IEEE 802.3-1998, Local and Metropolitan Area Networks-Specific Requirements-Part 3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications, and IEEE Std 802.3z-1998, Media Access Control (MAC) Parameters, Physical Layers, Repeater, and Management Parameters for 1000Mbps Operation, Type 1000BASE-X (Clauses 34-42) should be employed. The approved standard includes physical media types 1000Base-SX multi-mode fiber, 1000Base-LX single mode fiber, and 1000Base-CX. Work is continuing on 1000Base-T.*

### 3.4.2 Point-to-Point Standards

For full duplex, synchronous or asynchronous, point-to-point communication, the following standards are mandated:

- IETF Standard 51/RFC-1661/RFC-1662, Point-to-Point Protocol (PPP), July 1994.
- IETF RFC-1332, PPP Internet Protocol Control Protocol (IPCP), May 1992.
- IETF RFC-1989, PPP Link Quality Monitoring (LQM), August 1996.
- IETF RFC-1994, PPP Challenge Handshake Authentication Protocol (CHAP), August 1996.
- IETF RFC-1570, PPP LCP Extensions, January 1994.

The serial line interface shall comply with one of the following mandated standards:

- EIA/TIA-232-E, Interface Between Data Terminal Equipment and Data Circuit Terminating
- Equipment Employing Serial Binary Data Interchange, July 1991.
- EIA/TIA-530-A, High Speed 25-Position Interface for Data Terminal Equipment and Data Circuit

- Terminating Equipment, June 1992, Including Alternate 26-Position Connector, 1992. (This calls out EIA 422B and 423B.)

*Emerging: Point-to-Point Standards. IETF draft standard RFC 1990, PPP Multilink Protocol, allows for aggregation of bandwidth via multiple simultaneous dial-up connections. It proposes a method for splitting, recombining, and sequencing datagrams across multiple PPP links connecting two systems.*

### 3.4.3 Combat Net Radio Networking

CNRs are a family of radios that allow voice or data communications for mobile users. These radios provide a half-duplex, broadcast transmission media with potentially high Bit Error Rates (BERs). The method by which IP packets are encapsulated and transmitted is specified in MIL-STD-188-220B. With the exception of High Frequency (HF) networks, MIL-STD-188-220B shall be used as the standard communications net access protocol for CNR networks.

The following standard is mandated:

- MIL-STD-188-220B, Interoperability Standard for Digital Message Transfer Device (DMTD) Subsystems, 20 January 1998.

### 3.4.4 Integrated Services Digital Network

Integrated Services Digital Network (ISDN) is an international standard used to support integrated voice and data over standard twisted-pair wire. ISDN defines a Basic Rate Interface (BRI) and Primary Rate Interface (PRI) to provide digital access to ISDN networks. These interfaces support both circuit-switched and packet-switched services. It should be noted that deployable systems might additionally be required to support other non-North American ISDN standards when accessing region-specific international infrastructure for ISDN services. The JTA recognizes that this is a critical area affecting interoperability but does not recommend specific solutions in this version.

The following standards are mandated:

For BRI physical layer:

- ANSI T1.601, ISDN Basic Access Interface for Use on Metallic Loops for Application on the Network Side of the NT (Layer 1 Specification), 1992.

- ANSI T1.605, ISDN Basic Access Interface for S and T Reference Points - Layer 1 Specification, 1991.

For PRI physical layer:

- ANSI T1.408, ISDN Primary Rate – Customer Installation Metallic Interfaces (Layer 1 Specification), 1990.

For the data-link layer:

- ANSI T1.602, ISDN Data Link Signaling Specification for Application at the User Network Interface, 1996.

For signaling at the user-network interface:

- ANSI T1.607, Digital Subscriber Signaling System No. 1 (DSS1) - Layer 3 Signaling Specification for Circuit Switched Bearer Service, 1990.
- ANSI T1.610, DSS1 - Generic Procedures for the Control of ISDN Supplementary Services, 1994.
- ANSI T1.619, Multi-Level Precedence and Preemption (MLPP) Service, ISDN Supplementary Service Description, 1992.
- ANSI T1.619a, Supplement, 1994.

For signaling at node-to-node interface:

- ANSI T1.111, Signaling System No. 7, Message Transfer Part, 1996.
- ANSI T1.112, Signaling System No. 7, Signaling Connection Control Part Functional Description, 1996.
- ANSI T1.113, Signaling System No. 7, ISDN User Part, 1995.
- ANSI T1.114, Signaling System No. 7, Transaction Capability Application Part, 1996.

For signaling at the user-network interface, ANSI mandates shall be as profiled by the following National ISDN documents as adopted by the North American ISDN User's Forum (NIUF):

- SR-3875, National ISDN 2000,Telcordia (formerly Bellcore), May 1999.
- R-4620, 1999 Version of National ISDN Basic Rate Interface Customer Premise Equipment Generic Guidelines, Telcordia, December 1998.
- SR4619, 1999 Version of National ISDN Primary Rate Interface Customer Premise Equipment Generic Guidelines, Telcordia, December 1998.

For addressing:

- ITU-T E.164, Numbering Plan for the ISDN Era, May 1997.
- DISA Circular (DISAC) 310-225-1, Defense Switched Network (DSN) User Services Guide, 2 April 1998.

For transmitting IP packets when using ISDN packet-switched services:

- IETF RFC-1356, Multiprotocol Interconnect on X.25 and ISDN in the Packet Mode, 6 August 1992.

For transmitting IP packets using Point-to-Point Protocol (PPP) over ISDN:

- IETF RFC-1618, PPP over ISDN, 13 May 1994.

### *3.4.5 Asynchronous-Transfer Mode*

Asynchronous-Transfer Mode (ATM) is a high-speed switched data transport technology that takes advantage of primarily low bit error rate transmission media to accommodate intelligent multiplexing of voice, data, video, imagery, and composite inputs over high-speed trunks and dedicated user links. ATM is a layered type of transfer protocol with the individual layers

consisting of an ATM Adaptation Layer (AAL), the ATM layer, and the Physical Layer. The function of the AAL layer is to adapt any traffic (video streams, data packets from upper layer protocols) into the ATM format of 48-octet payload. It also receives the cells from the ATM layer and reassembles the protocol data units. The ATM Layer adds the necessary header information used by switches and end-systems alike to transfer cells across the ATM network. The Physical Layer converts the cell information to the appropriate electrical/optical signals for the given transmission medium. The ATM Forum's User-Network Interface (UNI) Specification defines the primary specification for end-system connection to ATM networks. The Private Network-Network Interface (PNNI) Specification defines the PNNI protocol for use between private ATM switches, and between groups of private ATM switches. The PNNI supports the distribution of topology information between switches and clusters of switches to allow paths to be computed through the network. The PNNI also defines the signaling to establish point-to-point and point-to-multipoint connections across the ATM network. ATM Forum's Local Area Network Emulation supports the emulation of Ethernet, allowing ATM Networks to be deployed without disruption of host network protocols and applications. For information on the ASD (C3I) ATM guidance, see URL:

http://www.disa.mil

The following standards are mandated:

For Physical Layer:

- ATM Forum, af-phy-0040.000, Physical Interface Specification for 25.6 Mbps over Twisted Pair Cable, November 1995.
- ATM Forum, af-uni-0010.002, ATM UNI Specification V 3.1, Section 2.1and 2.4, September 1994.
- ATM Forum, af-phy-0015.000, ATM Physical Medium Dependent Interface for 155 Mbps over Twisted Pair Cable, September 1994.
- ATM Forum, af-phy-0016.000, DS1 Physical Layer Specification, September 1994.
- ATM Forum, af-phy-0054.000, DS3 Physical Layer Interface Specification, January 1996.
- ATM Forum, af-phy-0046.000, 622.08 Mbps Physical Layer Specification, January 1996.
- ATM Forum, af-phy-0064.000, E-1 Physical Interface Specification, September 1996.
- ATM Forum, af-phy-0043.000, A Cell-based Transmission Convergence Sublayer for Clear Channel Interfaces, November 1995.

For User to Network Interface:

- ATM Forum, af-uni-0010.002, ATM UNI Specification V3.1, September 1994.
- ATM Forum, af-sig-0061.000, UNI Signaling Specification, Version 4.0, July 1996.

For Layer Management Capabilities:

- ATM Forum, af-ilmi-0065.000, Integrated Local Management Interface (ILMI) Specification, Version 4.0, September 1996.

- ATM Forum, af-uni-0010.002, ATM UNI Specification V 3.1, (Section 4:ILMI for UNI 3.1) September 1994.

For Traffic Management Functions:

- ATM Forum, af-tm-0056.000, Traffic Management Specification, Version 4.0, April 1996.

For Circuit Emulation Functions:

- ATM Forum, af-vtoa-0078.000, Circuit Emulation Service Interoperability Specification 2.0, January 1997.

For AAL1 and AAL5 Functions:

- ITU-T I.363.1, B-ISDN ATM Adaptation Layer Specification: Type 1 ATM Adaptation Layer (AAL1), August 1996.
- ITU-T I.363.5, B-ISDN ATM Adaptation Layer Specification: Type 5 ATM Adaptation Layer (AAL5), August 1996.

For Private Network-to-Network Interfaces:

- ATM Forum, af-pnni-0055.000, Private Network to Network Interface (PNNI) Specification, Version 1.0, March 1996.
- ATM Forum, af-pnni-0066.000, PNNI Specification, Version 1.0 Addendum (Soft PVC MIB), September 1996.

For Local Area Network Emulation and IP Over ATM:

- ATM Forum, af-lane-0021.000, Local Area Network Emulation (LANE) Over ATM, Version 1.0, January 1995.
- ATM Forum, af-lane-0038.000, LAN Emulation Client Management Specification, September 1995.
- ATM Forum, af-lane-0050.00, LANE Over ATM, Version 1.0 Addendum, December 1995.
- ATM Forum, af-lane-0057.000, LANE Servers Management Specification 1.0, March 1996.
- ATM Forum, af-mpoa-0087.000, Multi-Protocol Over ATM, Version 1.0, July 1997.

For ATM Addressing Format:

- DoD ATM Addressing Plan, 17 April 1998.

*Emerging: ATM-Related Standards. The ATM Forum has developed new Version 4.0 standards for signaling ABR addendum (af-sig-0076.000), and traffic management ABR addendum (af-tm-0077.000). Since ATM is essentially a packet- rather than circuit-oriented transmission technology, it must emulate circuit characteristics in order to provide support for CBR or "circuit" (voice and telephony) traffic over ATM. For voice and telephony, ATM trunking using AAL1 for Narrowband Services Version 1.0, af-vtoa-0089.000 was approved. For ATM security services, af-sec-0096.000, ATM Security Framework Specification, V1.0 was recently approved. For voice applications requiring bandwidth efficiency, af-vtoa-0113.000, ATM*

*Trunking Using AAL2 for Narrowband Services was recently approved. For bandwidth limited tactical interfaces, Low Speed Circuit Emulation Service, af-vtoa-0119.00, is emerging.*

*LANE Version 2.0 LANE UNI (LUNI) specification was recently approved by the ATM Forum. The LANE Version 2.0 LUNI, af-lane-0084.000, standardizes the interface between the LANE client (the LEC) and the LANE Server (the LES, LECS, and BUS).*

## *3.4.6 Satellite Communications*

Military Satellite Communications (MILSATCOM) systems include those systems owned or leased and operated by DoD and those commercial satellite communications (SATCOM) services used by DoD. The basic elements of satellite communications are a space segment, a control segment, and a terminal segment (air, ship, ground, etc.). An implementation of a typical satellite link will require the use of satellite terminals, a user communications extension, and military or commercial satellite resources.

### 3.4.6.1 Super High Frequency Satellite Terminal Standards Earth Terminals

For minimum mandatory Radio Frequency (RF) and Intermediate Frequency (IF) requirements to ensure interoperability of SATCOM Earth terminals operating over C-, X-, and Ku-band channels, the following standard is mandated:

- MIL-STD-188-164, Interoperability and Performance Standards for C-Band, X-Band, and Ku-Band SHF Satellite Communications Earth Terminals, 13 January 1995; with Notice of Change 1, 9 September 1998.

### 3.4.6.2 Phase-Shift Keying Modems

For minimum mandatory requirements to ensure interoperability of Phase-Shift Keying (PSK) modems operating in Frequency Division Multiple Access (FDMA) mode, the following standard is mandated:

- MIL-STD-188-165, Interoperability and Performance Standards for SHF Satellite Communications PSK Modems (Frequency Division Multiple Access (FDMA) Operations), 13 January 1995, with Notice of Change 1, 9 September 1998.

## *3.4.7 Personal Communications Services and Mobile Cellular.*

Personal Communications Services (PCS) will support both terminal mobility and personal mobility. Terminal mobility is based on wireless access to the public switched telephone network (PSTN). Personal mobility allows users of telecommunications services to gain access to these services from any convenient terminal (either wireline or wireless). Mobile cellular radio can be regarded as an early form of “personal communications service” allowing subscribers to place and receive telephone calls over the PSTN wherever cellular service is provided. There are three predominant competing worldwide methods for digital PCS and Mobile Cellular access: Code Division Multiple Access (CDMA), Time Division Multiple Access (TDMA), and Global System for Mobile Communications (GSM). Of these three, CDMA offers the best technical advantages for military applications based on its utilization of Direct Sequence Spread Spectrum (DSSS) techniques for increased channel capacity, low probability of intercept (LPI), and protection against jamming. CDMA's low transmission power requirements should also reduce portable

power consumption. The PCS standard for CDMA is J-STD-00. The Mobile Cellular standard for CDMA is TIA/EIA-95-B. In North America, the standard signaling protocol for CDMA and TDMA mobile cellular is TIA/EIA-41-D. It should be recognized that for Operations-Other-Than-War (OOTW), a user may require support of multiple protocols to access region-specific international digital PCS/Mobile Cellular infrastructures.

*Emerging: International Mobile Telecommunications – – 2000. International Mobile Telecommunications – – 2000 (IMT-2000) defines third-generation mobile systems scheduled to start service around the year 2000, subject to market conditions. Also known as Future Public Land Mobile Telecommunications Systems (FPLMTS), these systems will provide access by means of one or more radio links to a wide variety of telecommunication services supported by the fixed and mobile telecommunications networks (e.g., PSTN/ISDN) and to other services that may be unique to IMT-2000.*

*A range of mobile terminal types, designed for mobile and fixed use, is envisaged linking to terrestrial- and/or satellite-based networks. A goal for third-generation mobile systems is to provide global coverage and to enable terminals to be capable of seamless roaming between multiple networks. The ability to coexist and work with pre-IMT-2000 systems is required. Evaluation of the submitted IMT-2000 Radio Transmission Technologies (RTT) was completed 17 March 1999 and resulted in Recommendation ITU-R M. (IMT-RKEY) containing the key technical characteristics to be used in the IMT-2000 radio standard. IMT-RKEY was then used as input to begin developing Recommendation ITU-R M. (IMT-RSPC) on the radio interfaces for IMT-2000. The work is proceeding with the view of seeking a single standard for the terrestrial component of IMT-2000 encompassing two high-level technology groupings: CDMA and TDMA.*

*Determination of IMT-RSPC is expected by the end of 1999.*

## 3.5 Transmission Media – LANs/CANs

Transmission media refers to the physical media used to interconnect devices such as workstations, PCs, terminal, and telephones. Media my be channeled as in the case of copper, coaxial, and fiber optic cable, or unchanneled as in the case of the radio frequency spectrum.

Local Area Networks (LANs) and Campus Area Network (CAN) transmission media typically employ unshielded twisted pair (UTP) copper cabling and fiber optic media. Inter and intra-facility premises distribution system standards for local and campus area networks have been defined by the Telecommunications Industry Association (TIA)/Electronics Industry Association (EIA) for both UTP and fiber.

The following standards are mandated:

- TIA/EIA-568, Commercial Building Telecommunications Cabling Standard (ANSI/TIA/EIA-568-A-95), 25 October 1995.
- TIA/EIA-569, Commercial Building Standards for Telecommunications Pathways and Spaces (ANSI/TIA/EIA-569-A-98), 24 October 1990.

# 4. Presentation

The predominant types of HCIs include graphical user interfaces (GUIs) and character-based interfaces. For all DoD automated systems, the near-term goal is to convert character-based interfaces to GUIs. Although GUIs are the preferred user interface, some specialized devices may require use of character-based interfaces due to operational, technical, or physical constraints. These specialized interfaces shall be defined by domain-level style guides and further detailed in system-level user interface specifications. In order to present a consistent interface to the user, application software shall not mix command line user interfaces and GUIs.

## 4.1 Web Server

A Web server is a program that, using the client/server model and the World Wide Web's Hypertext Transfer Protocol (HTTP), serves the files that form Web pages to Web users (whose computers contain HTTP clients that forward their requests).

## 4.2 Character-Based Interfaces

The following, found at: <http://www-library.itsi.disa.mil/tafim.html> is mandated for systems with an approved requirement for a character-based interface:

- DoD Human Computer Interface Style Guide, 30 April 1996

While not mandated, additional guidance for developing character-based interfaces can be found in ESD-TR-86-278, Guidelines for Designing User Interface Software (Smith and Mosier 1986).

## 4.3 Graphical User Interfaces (GUI)

When developing DoD automated systems, the graphical user interface shall be based on one commercial user interface style guide. Hybrid GUIs that mix user interface styles (e.g., Motif with Microsoft Windows) shall not be created. A hybrid GUI is composed of toolkit components from more than one user interface style. When selecting commercial off-the-shelf (COTS)/Government off-the-shelf (GOTS) applications for integration with developed DoD automated systems, maintaining consistency in the user interface style is highly recommended. An application delivers the user interface style that matches the host platform (i.e., Motif on a UNIX platform and Windows on an NT platform). This style conforms to commercial standards, with consistency in style implementation regardless of the development environment used to render the user interface. Applications that use platform-independent languages such as Java deliver the same style as the native application on the host platform.

The following standards are mandated for use in UNIX/Motif Windows Manager environments:

- M021: CDE 2.1/Motif 2.1 User's Guide, ISBN 1-85912-173-X, October 1997.
- M027: CDE 2.1/Motif 2.1 - Style Guide and Glossary, ISBN 1-85912-104-7, October 1997.
- M028: CDE 2.1/Motif 2.1 - Style Guide Certification Check List, ISBN 1-85912-109-8, October 1997.

- M029: CDE 2.1/Motif 2.1 - Style Guide Reference, ISBN 1-85912-114-4, October 1997.
- M213: Motif 2.1 - Programmer's Guide, ISBN 1-85912-134-9, October 1997.
- M214A: Motif 2.1 - Programmer's Reference, Volume 1, ISBN 1-85912-119-5, October 1997.
- M214B: Motif 2.1 - Programmer's Reference, Volume 2, ISBN 1-85912-124-1, October 1997.
- M214C: Motif 2.1 - Programmer's Reference, Volume 3, ISBN 1-85912-164-0 October 1997.
- M216: Motif 2.1 - Widget Writer's Guide, ISBN 1-85912-129-2, October 1997.

The following standard is mandated for use with operating systems running (or intended to run) Win32 Applications:

- Win32 APIs, Window Management and Graphics Device Interface, Volume 1 Microsoft Win32 Programmers Reference Manual, 1993 or later, Microsoft Press.

## 4.4 Graphics Services

These services support the creation and manipulation of graphics. The following standards are mandated for non-COTS graphics development:

- ANSI/ISO/IEC 9636-1,2,3,4,5,6:1991 (R1997), Information Technology Computer Graphics Interfacing (CGI) Techniques for Dialogue with Graphics Devices.
- The OpenGL Graphics System: A Specification (Version 1.1) 25 June 1996 (for three-dimensional graphics).

# 5. Distributed Computing

These services allow various tasks, operations, and information transfers to occur on multiple physically or logically dispersed computer platforms. These services include, but are not limited to: global time; data, file, and name services; thread services; and remote-process services. There are two categories of Distributed-Computing Services: Remote-Procedure Computing and Distributed-Object Computing.

## 5.1 Remote-Procedure Computing

The mandated standards for remote-procedure computing are identified in the Open Group Distributed Computing Environment (DCE) Version 1.1.

The mandated standards are:

- C310, DCE 1.1: Time Services Specification, X/Open CAE Specification, November 1994.
- C311, DCE 1.1: Authentication and Security Services, Open Group CAE Specification, August 1997.
- C705, DCE 1.1: Directory Services, Open Group CAE Specification, August 1997.
- C706, DCE 1.1: Remote Procedure Call, Open Group CAE Specification, August 1997.

The C311 specification is included here to provide the complete definition of the DCE. Section 8, Security Services, specifies the other security requirements that must be met.

When used in conjunction with the POSIX Threads Extensions, the recommendations of the Open Group's Single UNIX Specification Version 2 -- 6 Vol. Set for UNIX 98 -- are expected to integrate the DCE thread model with the POSIX thread model.

## 5.2 Distributed-Object Computing

The mandate for distributed-object computing is interworking with the Object Management Group (OMG) Object Management Architecture (OMA), composed of the Common Object Request Broker Architecture (CORBA), CORBAservices, and CORBAfacilities. The CORBA specification defines the interfaces and services for Object Request Brokers, including an Interface Definition Language (IDL) and the Internet Inter-ORB Protocol (IIOP). CORBAservices define interfaces and semantics for services required to support distributed objects, such as naming, security, transactions, and events. CORBAfacilities defines interfaces and semantics for services required to support functions such as compound document manipulation. Interworking is the exchange of meaningful information between computing elements (semantic integration). Application-Level Interworking, for CORBA, results in CORBA clients interacting with non-CORBA servers and non-CORBA clients interacting with CORBA servers. For OLE/COM, Application-Level Interworking results in COM/OLE clients interacting with non-COM/OLE servers and non-COM/OLE clients interacting with COM/OLE servers.

The CORBA interoperability mandate does not preclude the use of other distributed-object technologies, such as ActiveX/DCOM or Java, as long as the capability for interworking with

CORBA applications and objects is maintained by the non-CORBA system. Products are available that allow interworking among distributed-object techniques.

Interworking with the following specification is mandated:

- The Common Object Request Broker: Architecture and Specification, Version 2.3, June 1999, OMG document formal/98-12-011 February 1998.

When a CORBA Object Request Broker (ORB) is used, the following specifications are mandated:

- Naming Service Specification: March 1995, contained in CORBAservices: Common Object Services Specification 05 July 1998.
- Event Service Specification: March 1995, contained in CORBAservices: Common Object Services Specification 05 July 1998.
- Transaction Service Specification: November 1997,contained in CORBAservices: Common Object Services Specification 05 July 1998.
- Time Service Specification: July 1997, contained in CORBAservices: Common Object Services Specification 05 July 1998.
- Trading Object Services Specification: March 1997,contained in CORBAservices: Common Object Services Specification 05 July 1998.

For DCE users that need to interwork with CORBA, the following standard is mandated:

- OMG document orbos/98-06-01, CORBAservices DCE/CORBA Interworking Service Negotiation Facility OMG ec/98-02-04.

For COM users that need to interwork with CORBA, the following standards are mandated:

- OMG document orbos/97-09-06, COM/CORBA Part B, Interworking, November 19, 1997.
- OMG document orbos/97-09-07, COM/CORBA Part A Revision November 19, 1997.

## 5.3 Middleware

Interprocess messaging is a middleware technology that uses message passing and message queuing to provide peer-to-peer asynchronous communication between programs. Messaging is a relatively mature technology that has been widely used for distributed applications involving high transaction rates in the banking, stock market, and airline industries. Few standards exist, however, for portable messaging APIs or interoperable messaging protocols.

In many implementations of messaging middleware, the basic message-passing model is enhanced with a message queue to provide a buffer for storing messages that have been sent and are waiting to be received. In this enhanced model, the send verb of the API becomes a put-on-queue operation, and the receive verb becomes a get-from-queue operation.

In contrast to other interprocess communication technologies, message queuing is inherently connectionless. In many message-queuing implementations, no direct connection is ever established between the application client and application server. With message queuing, the

sender and receiver do not need to be simultaneously available to communicate, nor does the network need to be available directly between the sender and receiver. This capability to support discontinuous communication makes message queuing more tolerant of a wide area network (WAN) than other interprocess communication technologies.

Message queuing has other characteristics that can be advantageous in specific application environments:

- Senders and receivers are not required to know each other.
- Messages can be processed in different sequences.
- Persistent queues can guarantee message delivery.
- Shared queues can support load balancing or parallel processing.

Final decisions regarding the adoption of standards will depend upon specific application architecture requirements for message queuing. A proposed ISO draft standard defines a model, an application layer service definition, and a protocol specification for message queuing. A proposed TOG draft standard defines a message-queuing API. If adopted, these standards may promote interoperability and source code portability between message-queuing products.

## 5.4 Transaction Processing

A key enabler of the *n*-tier computing model is a distributed transaction processing (DTP) capability. DTP systems provide the services required to manage and process distributed transactions in a heterogeneous computing environment. Common DTP services include concurrency control, failure isolation, dynamic load balancing, configuration management, message queue management, two-phase commit, and transactional RPC.

Choose a transaction monitor based on its capability to support widely accepted industry standards and the *n*-tier model of computing.

The following standards are mandated:

- X/Open C193: 1992, Distributed TP: The XA Specification
- X/Open S423: 1994, Distributed TP: The XA+ Specification, Version 2 (Based on CPI-C, Version 2)
- X/Open C504: 1995, Distributed TP: The TX (Transaction Demarcation) Specification
- X/Open C505: 1995, Distributed TP: The TxRPC Specification
- X/Open C506: 1995, Distributed TP: The XATMI Specification
- ISO/IEC 10026: 1998, Information Technology - Open Systems Interconnection - Distributed Transaction Processing

# 6. Collaborative Services

## 6.1 Video Teleconferencing

The ASD (C3I) mandated Federal Telecommunications Recommendation (FTR) 1080A-1998 Video Teleconferencing Profile identifies ITU-T H.320 as the key standard to provide interoperability between VTC terminal equipment, both point-to-point and multipoint configurations operating at data rates of 56-1,920 Kilobits per second (Kbps). ITU-T H.320, Narrow Band Visual Telephone Systems and Terminal Equipment, July 1997, is an umbrella standard of recommendations addressing audio, video, signaling, and control. Also in the FTR is ITU-T T. 120, Transmission Protocols for Multimedia Data, July 1996, which references a family of standards for applications implementing the features of audiographic conferencing, facsimile, still-image transfer, annotation, pointing, whiteboard, file transfer, audiovisual control, and application sharing.

For VTC units (VTUs) and Multipoint Control Units (MCUs) operating at data rates of 56-1,920 Kbps, except for operation over packet-based TCP/IP networks, the standards contained in FTR 1080A-1998, Appendix A (See Table 1) are mandated:

- FTR 1080A-1998, Appendix A, Video Teleconferencing Profile, October 1998.

**TABLE 1. ITU-T/EIA STANDARDS MANDATED IN FTR 1080A-1998, APPENDIX A**

| Standard | Description | Usage |
|---|---|---|
| H281 | Far-end camera control protocol for video conferences using H224 | VTU Multimedia |
| G.711 | Pulse code modulation 3.1 KHz to 48, 56, and 64 (narrowband speech mode) | VTU Audio |
| G.722 | Audio CODEC, 7 KHz at 48, 56, and 64 Kbps (wideband speech) | VTU/MCU Audio |
| G.728 | Audio CODEC 3.1 KHz at 16 Kbps (narrowband speech mode) | VTU/MCU Audio |
| H.231<br>H.243 | Multipoint control unit functional description<br>Procedure for establishing communication between three or more audiovisual terminals using digital channels up to 2 Mbit/s | MCU General<br>MCU General |
| EIA 422B | Electrical characteristics of balanced voltage digital interface circuits | VTU/MCU Encryption Interface |
| EIA-449 | General-purpose 37-position and 9-position interface for data terminal equipment and data circuit-terminating equipment employing serial binary data interchange | VTU/MCU Encryption Interface |
| H221 | Frame structure for 64 to 1920 Kbit/s channel in audiovisual services | VTU/MCU General |
| H230 | Frame-synchronous control and indication signals for audiovisual systems | VTU/MCU General |
| H242 | System for establishing communication between audio visual terminals using digital channels up to 2 Mbits/s | VTU/MCU General |
| H261 | Video CODEC for audiovisual services at px64 Kbps | VTU/MCU Video |
| H320 | Narrow-band visual telephone systems and telephone equipment | VTU/MCU General |
| T120 | Transmission protocols for multimedia data | VTU/MCU Multimedia |
| T122 | Multipoint communications service for audiographic and audiovisual conferencing service definition | VTU/MCU Multimedia |
| T123 | Protocol stacks for audiographic and audiovisual teleconferencing applications | VTU/MCU Multimedia |
| T124 | Generic conference control for audiographic and audiovisual | VTU/MCU Multimedia |

| | | |
|---|---|---|
| | terminals and multipoint control units | |
| T 125 | Multipoint communications service protocol specification | VTU/MCU Multimedia |
| T126 | Multipoint still image and annotation conferencing protocol specification | VTU Multimedia |
| T127 | Multipoint binary file transfer protocol | VTU Multimedia |
| T128 | Multipoint application sharing | VTU Multimedia |
| T4 | Group 3 facsimile - hardcopy representation | VTU Multimedia |
| T. 82 | Softcopy image compression (Joint Bi-level Image Experts Group [JBIG]) | VTU Multimedia |
| T. 81 | Softcopy color image compression (Joint Photographic Experts Group [JPEG]) | VTU Multimedia |
| H.224 | Real-time control protocol for simplex applications using the H.221 LSD/HSD/MLP channels | VTU Multimedia |

For applications implementing the features of audiographic conferencing, facsimile, still-image transfer, annotation, pointing, whiteboard, file transfer, audiovisual control, and application sharing, over LANs and at low bit rates (9.6-28.8 Kbps), the following standard is mandated:

- ITU-T T.120, Transmission Protocols for Multimedia Data, July 1996

For VTC terminals operating within Local Area Networks, the following standard is mandated:

- ITU-T H.323, Packet-based Multimedia Communications Systems, January 1998. For all other implementations of H.323, such as used over wide area networks where bandwidth, quality of service, and scalability may not be sufficient for IP-based video conferencing, see emerging standards paragraph 2.3.3.1.2.

For VTC terminals operating at low bit rates (9.6 to 28.8 Kbps) the following standard is mandated:

- ITU-T H.324, Terminal for Low Bit Rate Multimedia Communications, January 1998.

For inverse multiplexers connected to VTC terminals, and for VTC terminals with built-in inverse multiplexers, the following standard is mandated:

- ITU-T H.244, Synchronized Aggregation of Multiple 64 or 56 Kbps channels, July 1995.

For information on the ASD (C3I) VTC guidance and the Federal Telecommunications Recommendation FTR 1080A-1998 Video Teleconferencing Profile, see URL: http://www.ncs.gov/n6 and URL: disavtc.spawars.navy.mil .

*Emerging: There are three emerging standards for VTC over ATM.*

*H.310 includes underlying standards for video (MPEG2) and audio (MPEG1, MPEG2). H.310 can be used for high-quality VTC requiring > 2 Mbps infrastructure, but does not currently have much industry support.*

*H.321 specifies the operation of H.320 codecs over ATM using AAL-1 or AAL-5. H.321 uses Quality of Service to manage videoconferencing quality. It lacks industry wide support.*

*H.323 has the most industry support for VTC over ATM. It provides for two modes of operation over ATM: 1) IP over ATM media stream and 2) Real-Time Protocol (RTP) over ATM media stream transport (H.323 Annex C). Implementation of H.323 over non-LAN media (e.g., Metropolitan Area Networks (MANs) and WANs, such as the Internet, SIPRNET, JWICS, …) is still evolving.*

## 6.2 Workflow

Workflow management technology facilitates work-related processes within organizations. Workflow management often supports relatively static business processes such as purchase order and invoice processing. Workflow tools for such applications may tend to be "document-centric," that is, oriented toward handling a document through various stages of processing, presentation, and routing. A document-centric approach may also suit business processes such as engineering change orders. Some organizations may also wish to apply workflow technology in support of multi-level processes such as engineering product design. In that application workflow tools tend to be "process-centric," representing processes and how teams of people perform tasks in processes, which may involve processing of multiple documents. In any case, workflow management technology benefits business processes by making them more productive. As workflow applications continue to increase in sophistication, many workflow services are migrating into desktop applications. Electronic forms and e-mail applications, primary examples of this migration, offer rules-based routing of forms and messages.

No standards specific to workflow products exist today, but the Workflow Management Coalition (WfMC) is defining standard interfaces between workflow engines, workflow definition packages, management information tools, work list tools, and invoked applications. Despite the current work on defining these standards, wide supplier compliance is not expected in the short term. In general, workflow applications should use high-level application programming interfaces (APIs) to communicate with desktop applications and use industry standard relational databases as their data store. Select workflow automation tools that strategically align with the WfMC reference model and APIs.

# 7. Data Management

Central to most systems is the sharing of data between applications. The data management services provide for the independent management of data shared by multiple applications. These services support the definition, storage, and retrieval of data elements from Database Management Systems (DBMS).

## 7.1 Metadata

Metadata is additional, descriptive data that is collected and maintained to fully define the data used by an enterprise - it is data about data. DoD metadata requirements have been established for standardization of data definitions across systems and organization. This common understanding of the data will allow implementation of shared data environments and eliminate the need for each system to obtain and maintain a separate copy of the data.

The following standard is mandated for Metadata:

- DoD Manual 8320.1-M-1, DoD Data Standardization Procedures, April 1998

## 7.2 Database

Data management services give applications access to structured data in a distributed environment. The ANSI Structured Query Language (SQL) standard is the primary interface to relational databases, but the SQL Access standard extends this interface to access databases over a network.

Application code using Relational Database Management System (RDBMS) resources and COTS RDBMSs shall conform to the requirements of Entry Level SQL.

The following standard is mandated for any system using an RDBMS:

- ISO/IEC 9075: 1992 Information Technology – Database Language – SQL with amendment 1, 1996, as modified by FIPS PUB 127-2: 1993, Database Language for Relational DBMSs. (Entry Level SQL).

In addition, the SQL/Call Level Interface (CLI) addendum to the SQL standard provides a standard CLI between database application clients and database servers.

The following API is mandated for both database application clients and database servers:

- ISO/IEC 9075-3:1995 Information Technology – Database Languages – SQL – Part 3: Call-Level Interface (SQL/CLI).

The ISO/IEC 9075-3 mandate does not preclude the use of Open Database Connectivity (ODBC) 3.0 or JDBC extensions in situations where the capabilities supported by ISO/IEC 9075-3 cannot satisfy user functional requirements. Note that ISO/IEC 9075-3 is a subset of ODBC 3.0.

# 8. Security Services

Interoperability requires seamless information flow at all levels of information classification without compromising security. The goal is to protect information at multiple levels of security, recognizing that today' s DoD systems are "islands" of system-high solutions.

The concept of security assurance provides confidence that the security features do what they are supposed to do, and that they do not do what they are not supposed to do. While assurance has been largely associated with product security, it is an equally important concept applied to system security since it is unlikely that integrated products will retain their individual assurance characteristics.

DoD systems should have adequate safeguards to enforce DoD security policies and system security procedures. System safeguards should provide adequate protection from user attempts to circumvent system access control, accountability, or procedures for the purpose of performing unauthorized system operations.

The proper selection of standards can also provide a basis for improved information protection. Although few specific standards for the general topic of "information protection" exist within Defensive Information Warfare, selecting standards with security-relevant content contributes to the overall improvement of the security posture of information systems.

## 8.1 Application Environment

For the application environment, security standards are mandated for data management services and operating system services consistent with the required level of trust in accordance with DoDD 5200.28.

The following standard is mandated for data management services consistent with the required level of trust:

- NCSC-TG-021, Version 1, Trusted Database Management System Interpretation, April 1991.

The following standard is mandated for the acquisition of operating systems consistent with the required level of trust:

- DoD 5200.28-STD, The DoD Trusted Computer System Evaluation Criteria, December 1985.

If FORTEZZA services are used, the following standards are mandated:

- FORTEZZA Application Implementers' Guide, MD4002101-1.52, 5 March 1996.
- FORTEZZA Cryptologic Interface Programmers' Guide, MD4000501-1.52b, 20 October 1997.

*Emerging: The Generic Security Service-Application Program Interface (GSS-AP1), as defined in RFC-1508, September 1993 (IETF), provides security services to callers in a generic fashion, supportable with a range of underlying mechanisms and technologies and hence allowing source-level portability of applications to different environments. RFC-1508 defines GSS-API services and primitives at a level independent of an underlying mechanism and programming language*

*environment. RFC-2078, "GSS-API, Version 2.0," J. Linn, January 1997, revises RFC-1508, making specific, incremental changes in response to implementation experience and liaison requests.*

*The IETF Draft, "Independent Data Unit Protection Generic Security Service Application Program Interface (IDUP-GSS-API)," C. Adams, 25 March 1997, <draft-ietf-cat-idup-gss-07.txt>, extends the GSS-API (RFC-1508) for non-session protocols and applications requiring protection of a generic data unit (such as a file or message) independent of the protection of any other data unit and independent of any concurrent contact with designated "receivers" of the data unit. An example application is secure electronic mail in which data needs to be protected without any online connection with the intended recipient(s) of that data. Subsequent to being protected, the data unit can be transferred to the recipient(s)--or to an archive--perhaps to be processed as unprotected days or years later.*

*Distributed computing services security standards are also emerging. The Common Object Request Broker Architecture (CORBA) Security Services define a software infrastructure that supports access control, authorization, authentication, auditing, delegation, non-repudiation, and security administration for distributed-object-based systems. This infrastructure can be based on existing security environments and can be used with existing permission mechanisms and login facilities. The key security functionality is confined to a trusted core that enforces the essential security policy elements. Since the CORBA Security Services are intended to be flexible, two levels of conformance may be provided. Level 1 provides support for a default system security policy covering access control and auditing. Level 1 is intended to support applications that do not have a default policy. Level 2 provides the capability for applications to control the security provided at object invocation and also for applications to control the administration of an application-specific security policy. Level 2 is intended to support multiple security policies and to provide the capability to select separate access control and audit policies.*

## 8.2 Auditing and Alarm Reporting

Security auditing is a review or examination of records and activities to test controls, ensure compliance with policies and procedures, detect breaches in security, and indicate changes in operation. Security alarm reporting is the capability to receive notifications of security-related events; alerts of any misoperations of security services and mechanisms; alerts of attacks on system security; and information as to the perceived severity of any misoperation, attack, or breach of security.

The following standard is mandated for security auditing or alarm reporting:

- DoD 5200.28-STD, The DoD Trusted Computer System Evaluation Criteria, December 1985.

## 8.3 Authentication

Authentication supports tracing security-relevant events to individual users. If Open Software Foundation DCE Version 1.1 is used, the following authentication standard is mandated:

- IETF RFC-1510, The Kerberos Network Authentication Service, Version 5, 10 September 1993.

If DCE Version 1.1 is not used, the following authentication standard is mandated:

- FIPS-PUB 112, Password Usage, 30 May 1985.

Additional guidance documents: NC SC-TG-017 - A Guide to Understanding Identification and Authentication in Trusted Systems: CSC-STD-002 DoD Password Management Guidance.

*Emerging: IETF-RFC-2289, "A One-Time Password System," February 1998, provides authentication for system access (login)—and other applications requiring authentication—that is secure against passive attacks based on replaying captured reusable passwords. The One-Time Password System evolved from the S/KEY One-Time Password System released by Bellcore. Another emerging standard, IETF RFC 2138, "Remote Authentication Dial In User Service (RADIUS)," April 1997, supports Remote Dial-In Authentication.*

## 8.4 Encryption and Transmission

Encryption and transmission security standards include security algorithms, security protocols, and evaluation criteria. The first-generation FORTEZZA Cryptographic Card is designed for protection of information in messaging and other applications.

For systems required to interface with Defense Message System for Organizational Messaging, the following standards are mandated:

- FORTEZZA Interface Control Document, Revision P1.5, 22 December 1994.
- FI PS-PUB 140-1 Security Requirements for Cryptographic Modules, 11 January 1994.

### *8.4.1 Security Algorithms*

To achieve interoperability, products must support a common transport protocol. Transport protocols must agree on common cryptographic message syntax, cryptographic algorithms, and modes of operations (e.g., cipher block chaining). Transport protocols support negotiation mechanisms for selecting common syntax, algorithms, and modes of operation.

The following paragraphs identify security standards that shall be used for the identified types of cryptographic algorithms. If message digest or hash algorithms are required, Key Recovery will be implemented in a certificate management hierarchy. In FORTEZZA applications the following standards are mandated.

- Secure Hash Algorithm-1 (Federal Information Processing Standard (FIPS 180-1) April 1995). Note: The Hash function provides a check for data integrity.
- Digital Signature Standard (DSS) (FIPS 186-1) Digital Signature Algorithm (DSA), December 1998.
- SKIPJACK algorithm (FIPS-185) February 1994, NSA, R21-TECH 044-91,21 May 1991.
- Key Exchange Algorithm (KEA), NSA, R21-TECH-23-94, 12 July 1994.

NOTE: Both the Key Exchange Algorithm (KEA) and the SKIPJACK Algorithm (FIPS-185) were declassified on 23 June 1998.

### 8.4.2 Security Protocols

The following standard is mandated for DoD systems required to exchange security attributes; for example, sensitivity labels:

- MIL-STD-2045-48501, Common Security Label, 25 January 1995.

Establishment of a certificate and key management infrastructure for digital signature is required the proper creation, distribution, and revocation of end users' public-key certificates. The following standard is mandated:

- ITU-T Rec. X.509 (ISO/IEC 9594-8.2), Version 3, The Directory: Authentication Framework, 1997.

The Message Security Protocol (MSP) Version 4.0 has been revised to accommodate, in part, Allied requirements. All of MSP 4.0 features have been incorporated into ACP-120, Allied Communications Publication 120, Common Security Protocol. The following messaging security protocol is mandated for DoD message systems required to exchange sensitive but unclassified and classified information:

- ACP-120, Allied Communications Publication 120, Common Security Protocol (CSP), Rev A, 7 May 1998.

The following key management protocol is mandated:

- SDN.903, revision 3.2, Secure Data Network System (SDNS) Key Management Protocol (KMP), 1 August 1989.

*Emerging: In mid-1996, some significant improvements were proposed to the Secure/Multipurpose Internet Mail Extensions (S/MIME) messaging security protocol and the underlying encapsulation protocol, PKCS#7. With these improvements, S/MIME will provide a business-quality security protocol for both the Internet and X.400 messaging environments. These improvements effectively merge S/MIME and Message Security Protocol (MSP) 4.0/ACP-120.*

### 8.4.3 Network Security

Systems processing classified information must use Type 1 NSA-approved encryption products to provide both confidentiality and integrity security services within the network.

When network-layer security is required, the following security protocol is mandated:

- SDN.301, Revision 1.5, Secure Data Network System (SDNS) Security Protocol 3 (SP3), 1989.

The following standard is mandated for DoD systems required to exchange security attributes; for example, sensitivity labels:

- MIL-STD-2045-48501, Common Security Label, 25 January 1995.

*Standards are emerging for Local Area Network (LAN) security and Metropolitan Area Networks (MANs) security. IEEE 802.10, Interoperable LAN/MAN Security (SILS) 1998, provides specification for an interoperable data link layer security protocol and associated security*

*services. It discusses services, protocols, data formats, and interfaces to allow IEEE products confidentiality. A security label option is specified that enables rule-based access control to be implemented using the Security Data Exchange (SDE) protocol. Key management on IEEE 802 Local Area Networks (LANs) and Metropolitan Area Networks (MANs) is described and published separately as IEEE 802.10c-1998.*

*RFC-2228, File Transfer Protocol, October 1997, defines extensions to the FTP standard (STD9/ RFC 959). These extensions provide strong authentication, integrity, and confidentiality on both the control and data channels. RFC-2228 also introduces new optional commands, replies, and file transfer encodings.*

### *8.4.4 Web Security*

The Secure Sockets Layer (SSL) protocol allows client/server applications to communicate in a way designed to prevent eavesdropping, tampering, or message forgery. It is currently the defacto standard used by most browsers and popular email packages that are associated with the browser. RFC 2246, The TLS Protocol Version 1.0, January 1999, is an Internet Engineering Task Force (IETF) Proposed Standard and is expected to supercede SSL as a mandated standard within 2 years. Since Netscape is supporting TLS development, it is expected that there will be no further development of the SSL protocol by Netscape. The following standard is mandated:

- Secure Sockets Layer (SSL) Protocol Version 3.0, 18 November 1996.

*Emerging: RFC 2246, The Transport Layer Security (TLS) Protocol Version 1.0, January 1999, is an Internet Engineering Task Force (IETF) Proposed Standard that provides communications privacy over the Internet. The protocol allows client/server applications to communicate in a way designed to prevent eavesdropping, tampering, or message forgery. It is based on the SSL 3.0 Protocol Specification as published by Netscape. TLS is expected to supercede SSL as a mandated standard within 2 years.*

*Pervasive use of the internet and internet related technologies has continued to raise issues related to security. The IETF collaborative process is addressing these issues through Requests for Comments (RFCs). Many standards are emerging from these efforts. They are discussed below.*

*RFC 2401, "Security Architecture for the Internet Protocol," S. Kent and R. Atkinson, November 1998, describes the security mechanisms for IP and the services that they provide. RFC-2401 also describes key management requirements for systems implementing those security mechanisms. This RFC specifies the base architecture for IPsec-compliant systems. It also describes the security services offered by the IPsec protocols and how these services can be employed in the IPv4 and IPv6 environments.*

*The Internet Draft RFC 2402, "IP Authentication Header," S. Kent and R. Atkinson, November 1998, describes a mechanism for providing integrity and authentication for IP datagrams. The IP Authentication Header (AH) is used to provide connectionless integrity and data origin authentication for IP datagrams, and to provide protection against replays.*

*RFC 2406, "IP Encapsulating Security Payload (ESP)," S. Kent and R. Atkinson, November 1998, discusses a mechanism for providing integrity and confidentiality to IP datagrams. In some circumstances, depending on the encryption algorithm and mode used, it can also provide*

*authentication to IP datagrams. Otherwise, the IP AH may be used in conjunction with ESP to provide authentication. The mechanism works with both IPv4 and lPv6.*

*RFC 2104, "HMAC: Keyed-Hashing for Message Authentication," February 1997, H. Krawczyk (IBM), M. Bellare (UCSD), R. Canetti (IBM). This document describes HMAC, a mechanism for message authentication using cryptographic hash functions. HMAC can be used with any iterative cryptographic hash function, e.g., MD5, SHA-1, in combination with a secret shared key. The cryptographic strength of HMAC depends on the properties of the underlying hash function.*

*RFC 1829, "The ESP DES-CBC Transform," P. Karn (Qualcomm), P. Metzger (Piermont), W. Simpson (Daydreamer), August 1995. This specification describes the ESP use of the Cipher Block Chaining (CBC) mode of the U.S. Data Encryption Standard (DES) algorithm (FIPS-46, FIPS-46-1, FIPS-74, FIPS-81).*

*Draft FIPS-PUB 46-3 Data Encryption Standard (DES). For those systems required or desiring to use a cryptographic device to protect privacy act information and other unclassified, non-Warner Act exempt information, the Data Encryption Standard (DES) may apply. The DES is found in draft FIPS PUB 46-3 Data Encryption Standard. RFC 2420, "The PPP Triple-DES Encryption Protocol (3DESE)", is a complement to FIPS 46-3.*

*IETF RFC-2065, "DNS Security Extensions," D. Eastlake, C. Kaufman, January 1997, describes extensions to the DNS that provide data integrity and authentication services to security-aware resolvers or applications through the use of cryptographic digital signatures. The extensions also provide for the storage of authenticated public-keys in the DNS. This storage of keys can support general public-key distribution service as well as DNS security.*

*IETF RFC 2408 "Internet Security Association and Key Management Protocol (ISAKMP)," Douglas Maughan, Mark Schertler, Mark Schneider, Jeff Turner, 21 February 1998, defines a framework for security association management and cryptographic key establishment for the Internet. It is expected that the IETF will adopt this protocol as the Internet standard for key and security association management for IPv6 security.*

*The IETF Draft, "The Resolution of ISAKMP with Oakley," D. Harkins, D. Carrel (Cisco Systems), February 1997, <draft-ietf-ipsec-isakmp-oaklev-03.txt>, describes a proposal for using the Oakley Key Exchange Protocol in conjunction with ISAKMP to obtain authenticated keying material for use with ISAKMP. Oakley describes a series of key exchanges--called "modes"--and details the services provided by each (e.g., perfect forward secrecy for keys, identity protection, and authentication).*

*RFC 2407, "The Internet IP Security Domain of Interpretation for ISAKMP," D. Piper, November 1998, details the Internet IP Security DOI, which is defined to cover the IP security protocols that use ISAKMP to negotiate their security associations.*

## 8.5 Evaluation Criteria

The following standards are mandated consistent with the required level of trust:

- DoD 5200.28-STD, The DoD Trusted Computer System Evaluation Criteria, December 1985.
- NCSC-TG-005, Version 1, Trusted Network Interpretation, July 1987.

*Emerging: The Evaluation Criteria for Information Technology Security (Common Criteria) represents the international community. It is an alignment and development of a number of the existing European, U.S., and Canadian criteria (ITSEC, TCSEC, and CTCPEC respectively). The Common Criteria resolves the conceptual and technical differences between the source criteria. It is a contribution to the development of an international standard, and it opens the way to worldwide mutual recognition of evaluation results. The ISO National Body approved ISO FDIS 15408, Common Criteria, Version 2.0, October 1998, in June 1999. The standard will be published in early Fall 1999.*

## 8.6 Public Key Infrastructure

A public-key infrastructure (PKI) comprises the people, policies, procedures, and computing/ telecommunications resources needed to manage public keys used by information systems. A PKI supports the following security services: authentication, data integrity, non-repudiation, confidentiality, and (optionally) authorization.

A PKI supports "X509 public-key certificates," as defined in International Telecommunications Union - Telecommunications (ITU-T) Recommendation X. 509. A public-key certificate is a data structure that binds a subject (people, applications programs, machines, etc) and the subject's public key. A public-key certificate may contain additional attributes of the subject, such as address, phone number, and authorization (access control) data.

A PKI may support X.509 attribute certificates. An attribute certificate binds a subject and the subject's authorization data, such as group membership, roles, clearances, privileges, and restrictions. The authorization data does not guarantee access to information resources, as the decision to grant or deny access is made by the application that uses the certificate. Attribute certificates do not contain public keys.

A private-key is used to digitally sign data, such as messages, files, and transactions. The corresponding public key is used to verify the signature. A private key can also be used to decrypt data encrypted with the corresponding public key. In the DOD medium-assurance PKI, the public/ private-key pairs used for non-repudiation or digital signature services will be distinct from the pairs used for encryption/decryption services. Public/private-key pairs are also used in algorithms that automatically distribute symmetric, secret keys.

X.509 public-key certificates are signed and issued by a special user called a certification authority (CA). A CA may also revoke certificates. X.509 attribute certificates are signed, issued, and revoked by an attribute certificate issuer.

The DoD medium-assurance PKI is authorized to protect unclassified and certain types of sensitive but unclassified (SBU) information, in accordance with the DoD Class 3 level of information assurance. The DoD medium-assurance PKI may also be used for digital signature services, user authentication, and community of interest separation within certain types of classified networks protected by Type I cryptography. The U.S. DoD X.509 Certificate Policy specifies the permitted uses of a medium-assurance (Class 3) PKI in encrypted and unencrypted networks.

The standards related to PKI are all emerging at this time. However, those listed below are the ones actually being used in the DoD medium-assurance pilot PKI. The standards are grouped according to the categories defined in the Internet Draft entitled "Internet X. 509 Public Key Infrastructure PKIX Roadmap", <draft-ietf-pkix-roadmap-02.txt>, 23 June 1999, plus additional

categories not mentioned in the Roadmap. Additional information on PKI policy can be found at http://www-pki.itsi.disa. mil/policy.htm.

### 8.6.1 Certificate Profiles

The DoD medium-assurance certificate profile implements the Federal PKI certificate profile, which in turn implements the Internet Engineering Task Force (IETF) profile, which in turn implements the ITU-T X.509 profile.

*Emerging: The following certificate profile standards are emerging: International Telecommunications Union -Telecommunications (ITU-T) Recommendation X.509, "Information Technology -Open Systems Interconnection -The Directory: Authentication Framework," June 1997 as profiled by RFC 2459, "Internet X.509 Public Key Infrastructure Certificate and CRL Profile," January 1999, IETF Proposed Standard, Federal Public Key Infrastructure Technical Working Group (FPKITWG) document TWG-98-07, "Federal PKI X.509 Certificate and CRL Extensions Profile," 9 March 1998; and DOD Certificate Profile, as defined in MITRE Technical Report 98W, "Department of Defense (DOD) Medium Assurance Public Key Infrastructure (PKI) Functional Specification (Draft),"Version 0.3, 20 October 1998, Appendices A-D.*

When DoD develops its Class 3 PKI interface specification, the DoD certificate profile will be included in it. MITRE Technical Report 98W is the only existing document that defines the DoD certificate profile.

### 8.6.2 Operational Protocols and Exchange Formats

Operational protocols deliver certificates and certificate revocation lists (CRLS) to certificate-using systems. The medium-assurance pilot uses RFC 2559, a profile of RFC 1777, Lightweight Directory Access Protocol, version 2, (LDAPv2), as its operational protocol.

*Emerging: RFC 2559, "Internet X.509 Public Key Infrastructure Operational Protocols: LDAPv2," April 1999, IETF Proposed Standard.*

*Certificates and CRLs are stored in LDAP servers, which are accessed by certificate-using systems through LDAPv2. RFC 2587 specifies the minimal schema required to support certificates and CRLs in an LDAP server. An emerging standard for LDAP PKI servers is RFC 2587, "Internet X.509 Public Key Infrastructure LDAPv2 Schema," June 1999, IETF Proposed Standard.*

*Certificates, private keys, and other personal data must be protected when they are moved between computers or removable media, such as smart cards or floppy disks. For secure or authenticated exchange of such personal data, the following standard is emerging: RSA Laboratories Public Key Cryptography Standard #12, "Personal Information Exchange Syntax Standard," version 1.0 (Draft), 30 April 1997.*

### 8.6.3 Management Protocols

Management protocols support transactions involving management entities, such as CAs, Registration Authorities (RAs), and Local Registration Authorities (LRAs). Typical transactions are user registration, certificate enrollment, and certificate revocation.

*Emerging: The following standards are emerging: RFC 2315, Public Key Cryptography Standard (PKCS) #7, Cryptographic Message Syntax, Version 1.5, March 1998, Informational RFC; and RFC 2314, PKCS #10, Certification Request Syntax, Version 1.5, March 1998, Informational RFC.*

*Although RFC 2315 and 2314 are based upon de facto standards from RSA Laboratories, Inc, the IETF is incorporating them into open, consensus-based standards, such as the Internet draft for "Certificate Management Messages over Cryptographic Message Syntax (CMC)." As the CMC draft matures, it will be considered for adoption as an emerging standard.*

### 8.6.4 Application Program Interfaces (APIs)

AP1 standards allow programmers to incorporate PKI services into their applications in a manner that supports applications portability.

*Emerging: The following standard is emerging: RSA Laboratories Public Key Cryptography Standard (PKCS) #11,"Cryptographic Token Interface Standard," version 1.0, 28 April 1995.*

### 8.6.5 Cryptography

*The following standards are emerging:*

*RSA Laboratories Public Key Cryptography Standard (PKCS) #1, "RSA Cryptography Standard," Version 2.0, 1 October 1998.*

*FIPS 140-1 "Security Requirements for Cryptographic Modules," 11 January 1994. {DOD X.509 Certificate Policy specifies the FIPS 140-1 security levels required for PKI users, RAs, and CAs}.*

*Draft FIPS 46-3, "Data Encryption Standard," 8 January 1999. (This replaces DES with Triple DES, as specified in ANSI X9.52)*

*The following standard is emerging for PKI Class 3 implementations: Federal Information Processing Standard (FIPS) 180-1, "Secure Hash Algorithm," April 1995.*

# 9. Application Management

## 9.1 Software Engineering

The software engineering services provide system developers with the tools that are appropriate to the development and maintenance of applications. There are no mandated standards for this service area. Language services provide the basic syntax and semantic definition for use by developers to describe the desired software function. "Programming language selections should be made in the context of the system and software engineering factors that influence overall life-cycle costs, risks, and potential for interoperability." Computer languages should be used in such a way as to minimize changes when compilers, operating systems, or hardware change. To maximize portability, the software should be structured where possible so it can be easily ported.

## 9.2 Activity Model

Activity models are used to document/model the activities, processes, and data flows supporting the requirements of process improvement and system development activities. Prior to system development or major system update, an activity model is prepared to depict the mission-area activity. The activity model can form the basis for data and/or object model development or refinement. It is validated against the requirements and doctrine, and approved by the operational sponsor. IEEE P1320.1, IDEF0 Function Modeling, is the standard that describes the IDEF0 modeling language semantics and syntax, and associated rules and techniques, for developing structured graphical representations of a system or enterprise.

The mandated standard for activity modeling is:

- IEEE 1320.1-1998, IEEE Standard for Functional Modeling Language—Syntax and Semantics for IDEF0.

## 9.3 Data Model

Relational data models are used in software requirements analyses and design activities as a logical basis for physical data exchange and shared data structures that can benefit from a relational schema definition, including message formats and schema for shared databases. Object-oriented systems use data models to design relational data structures when there is a requirement to maintain persistent data storage for that system in a relational database. IDEF1X is used to produce a graphical information model, which represents the structure and semantics of information within an environment or system. FIPS Pub 184 is the standard that describes the IDEF1X modeling language (semantics and syntax) and associated rules and techniques, for developing a logical model of data. Use of this standard permits the construction of semantic data models, which support the management of data as a resource, the integration of information systems, and the building or relational databases. System engineering methodology internal to a system is unrestricted.

The mandated standard for Data Modeling is:

- DoD Manual 8320.1-M-1, DoD Data Standardization Procedures, April 1998 (which mandates the use of the DDM).

- FIPS PUB 184, Integration Definition For Information Modeling (IDEF1X), December 1993.

### 9.3.1 Object Modeling

Object models define the combined information and process requirements within a domain needed to accomplish a particular capability or set of capabilities, for example, as defined by activity models. Such models form the basis of object-oriented system implementations. They also model system interoperability by combining the metadata for shared data with the allowable interfaces for sharing that data. Such models show associations and dependencies between system interfaces and the essential business rules for exercising those relationships. Object-oriented modeling techniques are used in the specification and development of object-oriented systems and to model and design the interoperability requirements of distributed components.

*Emerging: The emerging standards for object modeling are IDEF1X97, Conceptual Schema Modeling and the Unified Modeling Language (UML) Version 1.3.*

## 9.4 DoD Data Definitions

The Defense Data Dictionary System (DDDS) is a central database that includes standard data entities, data elements, and provides access to DDM files from the DDDS server. The procedures for preparing and submitting data definitions and data models for standardization are covered in DoD Manual 8320.1-M-1. A classified version of the DDDS, Secure Intelligence Data Repository (SIDR), has been developed to support standardization of classified data elements and domains. System developers shall use these repositories as a primary source of data element standards.

The mandated standards for DoD Data Definitions are:

- DoD Manual 8320.1-M-1, DoD Data Standardization Procedures, April 1998.

# 10. Information Exchange

Information-Exchange Standards refer to the exchange of information among mission-area applications within the same system or among different systems. The scope of information-exchange standards follows:

- The exchange of information among applications using shared databases or formatted message structures shall be based on the logical data models developed from identifying information requirements through activity models, where appropriate. The data model identifies the logical information requirements, which shall be developed into physical database schemata and standard data elements.
- The standard data elements shall be exchanged using the data-management, data interchange, and distributed-computing services of application platforms. The goal is to exchange information directly between information systems, subject to security classification considerations.
- Information exchange between systems using object-oriented interface definitions can be based on object models depicting those interfaces and the functional dependency of those interfaces. With object models, standard data elements are typically associated with the atomic data attributes that represent shared data.

Interchange standards help form the Defense Information Infrastructure (DII) Common Operating Environment (COE), ensuring the use of system or application formats that can share data. Key references include Section 7.2, for SQL standards in Data Management Services. In distributed databases, other types of data messaging may be used as long as they remain DDDS-compliant as discussed in Section 9.4.

## 10.1 Data Interchange Services

The data interchange services provide specialized support for the exchange of data and information between applications and to and from the external environment. These services include document, graphics data, audio data, and video data.

### 10.1.1 Document

The Standard Generalized Markup Language (SGML) format supports the production of documents intended for long-term storage and electronic dissemination for viewing in multiple formats. SGML formalizes document mark-up, making the document independent of the production and/or publishing system. SGML is an architecture-independent and application-independent language for managing document structures. SGML is a meta-language, providing the rules for designing and applying a system of markup tags rather than the specific set of tags.

The following standard is mandated:

- ISO 8879: 1986, Information processing -- Text and office systems -- Standard Generalized Markup Language (SGML) with Amendment 1, 1998.

The Hypertext Markup Language (HTML) is used for hypertext-formatted and navigational-linked documents. For hypertext documents intended to be interchanged via the Web or made available via organizational intranets, the following standard is mandated:

- HTML 4.0 Specification, W3C Recommendation, revised on 24-Apr-1998, REC-html40-19980424 <**http://www.w3.org/TR/1998/REC-html40-19980424**>.

The eXtensible Markup Language (XML) is a meta-language, based on SGML, for describing languages based on name-attribute tuples. This allows new capabilities to be defined and delivered dynamically.

For domain- and application-specific markup languages defined through tagged data items, the following is a mandated standard:

- Extensible Markup Language (XML) 1.0. W3C Recommendation, 10 February 1998. Reference: REC-xml-19980210, <**http://www.w3.org/TR/1998/REC-xml-19980210**>.

Continuous Acquisition and Life-Cycle Support (CALS) has developed a set of standards that apply to this service area. CALS Standard Generalized Markup Language (SGML) profiles the ISO standard (8879) by selecting a particular Document Type Definition (DTD) and other parameters that help standardize the development of technical manuals for DoD. CALS also developed a handbook for applying CALS SGML (MIL-HDBK-28001, 30 June 1995). Although Hypertext Markup Language (HTML) is also a subset of SGML, it is not sufficiently robust enough for TM development. (eXtensible Markup Language (XML) may replace both CALS SGML and HTML in the future.) CALS also has a standard for archiving documents (1840C).

The mandated standards for the CALS Document Interchange Service Area are:

- MIL-PRF-28001C, Markup Requirements and Generic Style Specification for Electronic Printed Output and Exchange of Text. (CALS SGML), 2 May 1997.
- MIL-STD-1840C, Automated Interchange of Technical Information (AITI), 26 June 1997.

Table 2 identifies file formats for the interchange of common document types such as text documents, spreadsheets, and presentation graphics. Individual vendors control some of these formats, but all of these formats are supported by products from multiple companies. In support of the standards mandated in this section, Table 2 identifies conventions for file name extensions for documents of various types. If an organization has a requirement for a given document type, the following file formats are mandated, but not the specific products mentioned:

- All applications acquired or developed for the production of documents shall be capable of generating at least one of the formats listed in Table 2 for the appropriate document type.
- The organization shall at a minimum be capable of reading and printing all of the formats listed below for the appropriate document type.

**TABLE 2. COMMON FILE INTERCHANGE FORMATS**

| File Type | Standard/Vendor Format | Recommended File Name Extension | Reference |
|---|---|---|---|
| Plain Text | ASCII Text | .txt | ISO/IEC646: 1991IRV |
| Compound Document | PDF 4.0 | .pdf | Vendor |
| | HTML 4.0 | .htm | W3C |
| | MS Word 97 | .doc | Vendor |
| | Rich Text Format | .rtf | Vendor |
| Briefing - Graphic Presentation | MS PowerPoint 97 | .ppt | Vendor |
| Spreadsheet | MS Excel 97 | .xls | Vendor |
| Database | Dbase 4.0<br>MSAccess 97 | .dbf<br>.mda, .mdb, .mbe | Vendor<br>Vendor |
| Compression | Zip file format | .zip | Vendor |

### *10.1.2 Graphics Data*

These services are supported by device-independent descriptions of the picture elements for vector and raster graphics. The International Organization for Standardization (ISO) Joint Photographic Expert Group (JPEG) standard describes several alternative algorithms for the representation and compression of raster images, particularly for imagery; JPEG images may be transferred using the JPEG File Interchange Format (JFIF). Graphics Interchange Format (GIF) and JFIF are de facto standards for exchanging graphics and images over an internet. GIF supports lossless compressed images with up to 256 colors and short animation segments. Note that Unisys owns a related patent, which requires a license for software that writes the GIF format. Portable Network Graphics (PNG) is an extensible file format for the lossless, portable, well-compressed storage of a raster image. Indexed-color, grayscale, and true color images are supported, plus an optional alpha channel for transparency. The PNG specification was issued as a W3C Recommendation on 1 October 1996.

For the interchange of very large still-raster images that have no geospatial context and where lossy decompression is acceptable, the mandate is:

- JPEG File Interchange Format, Version 1.02, September 1, 1993, C-Cubed Microsystems.

For the interchange of other single raster images that have no geospatial context and where lossy compression is not acceptable, the mandate is:

- PNG (Portable Network Graphics) Specification, W3C Recommendation REC-png.html http://www.w3.org/TR/REC-png.htm**.**

For the lossless interchange of raster images that have no geospatial context and where none of the above cases apply, such as the exchange of still-images that can be viewed in sequence (also referred to as animation), the mandate is:

- Graphics Interchange Format (GIF), Version 89a, 31 July 1990, CompuServe Incorporated.

The mandated standards for the CALS Graphics Data Interchange service area are:

- ANSI/ISO/IEC 8632 Information Technology - Computer Graphics - Metafile for the Storage and Transfer of Picture Description Information [part 1:1992 Functional Specifications (with amendment 1:1994 Rules for Profiles and with amendment 2:1995 Application Structuring Extensions)] and [part 3:1992 Binary Coding (with amendment 1:1994 Rules for Profiles and with amendment 2:1995 Application Structuring Extensions)] as profiled by MIL-PRF-28003A dated 15 November 1991 with Amendment 1 dated 14 August 1992, Performance Specification, Digital Representation for Communications of Illustration Data: CGM Application Profile.
- MIL-PRF-28002C, Performance Specification, Requirements for Raster Graphics
- Representation in Binary Format, 30 September 1997.

### *10.1.3 Audio Data*

Effective compression of audio data depends not only upon data compression techniques but also upon the application of a psycho-acoustic model that predicts which sounds humans are likely to be able to hear or not hear in given situations. The sounds selected for elimination depend on the bit rate available for streaming the audio data when the file is decoded and played. Therefore, the best selection of a file format depends upon the bandwidth assumed to be available on the platform that will decode the file.

For audio files intended to be decoded in an environment with a target bit rate of about 56 to 64 kilobits per second (Kbps) per audio channel, the following standards are mandated:

- ISO/IEC 11172-1: 1993 Information technology – Coding of moving pictures and associated audio for digital storage media at up to about 1.5 Mbit/s – Part 1: Systems, 1993; with Technical Corrigendum 1:1995.
- ISO/IEC 11172-3: 1993, Information technology – Encoding of moving pictures and associated audio for digital storage media at up to about 1.5 Megabits per second (Mbit/s) – Part 3 (Audio Layer-3 only); with Technical Corrigendum 1:1996.

### *10.1.4 Video Data*

MPEG-1 is an open international standard for video compression that has been optimized for single- and double-speed CD-ROM data transfer rates. The standard defines a bit-stream representation for synchronized digital video and audio, compressed to fit into a bandwidth of 1.5 Mbps. This corresponds to the data retrieval speed from CD-ROM and Digital Audio Tape (DAT). With 30 FPS video at a display resolution of 352 x 240 pixels, the quality of compressed and decompressed video at this data rate is often described as similar to that of a VHS recording. A major application of MPEG is the storage of audiovisual information on CD-ROM and DAT. MPEG is also gaining ground on the Internet as an interchange standard for video clips because the shell format is interoperable across platforms and considered to be platform-independent.

The following standards are mandated:

- ISO/IEC 11172-1: 1993, Information technology – Coding of moving pictures and associated audio for digital storage media at up to about 1.5 Mbits/s – Part 1: Systems, 1993; with Technical Corrigendum 1:1995.

- ISO/IEC 11172-2: 1993 Information technology – Coding of moving pictures and associated audio for digital storage media at up to about 1.5 Mbit/s – Part 2 Video; 1993.

MPEG-2 Main Profile @ Main Level (MP@ML) 4:2:0 systems are fully backward compatible with the MPEG-1 standard. MPEG-2 MP@ML can be used with all video support systems (storage, broadcast, network) at bit rates from 3 to 10 Mbps, where limited additional processing is anticipated, operating in either progressive or interlaced scan mode, optimally handling the resolution of the ITU-R 601 recommendation (i.e., 720 x 480 pixels for the luminance signal and 360 x 480 pixels for the color space).

The following video support standards for compressed video are mandated:

- ISO/IEC 13818-1: 1996, Information Technology – Generic Coding of Moving Pictures and Associated Audio Information – Part 1: Systems (MPEG-2); 1996, with Amendment 1:1997.
- ISO/IEC 13818-2: 1996 – Generic Coding of Moving Pictures and Associated Audio Information – Part 2: Video (MPEG-2); 1996, with Amendment 1:1997 and Amendment 2:1997. (The identical text is also published as ITU-T Rec. H.262.)

For information on Video Teleconferencing, see section 6.1,Video Teleconferencing.

### *10.1.5 Product Data*

Several standards exist for exchanging product data. The ANSI/US PRO/IPO-100-1993 and MIL-PRF-28000A standards for Initial Graphics Exchange Specification (IGES), define a neutral data format that allows the digital exchange of information between Computer-Aided Design (CAD) and Computer-Aided Manufacturing (CAD/CAM) systems. IGES supports digital design and manufacturing information about an object sufficient to support manufacturing and construction only. MIL-PRF-28000A contains applications subsets and protocols that form profiles of IGES Version 4.0.

The following standards are mandated:

- ANSI/US Product Data Association (PRO)-100-1993, Initial Graphics Exchange Specification (IGES), V5.3, 23 September 1996.
- MIL-PRF-28000A with Amendment 1, Digital Representation for Communications of Product Data: IGES Application Subsets and IGES Application Protocols, 14 December 1992.

Bar code standards are used to identify packages and products. They can be used to help identify products being shipped and stocked. MIL-STD-1189B was canceled but the notice directed the user to AIM BC-1, a linear bar code standard. Linear bar codes such as AIM BC-1 have limited storage capability, typically a maximum 17 characters. A two-dimensional material-handling standard was developed to allow for greater storage, up to 1850 characters. 2D bar codes can also sustain considerable damage and still be read. ANSI MH10.8.3M describes the use of two-dimensional symbols (e.g., PDF-417) in conjunction with unit loads and transport packages to convey data between trading partners. Additionally, it specifies the structure, syntax, and coding of dates when using two-dimensional symbols.

The following standards are mandated:

- AIM-BC 1095, Uniform Symbology Specification Code 39, 16 August 1997.
- PDF-417 as profiled by ANSI MH10.8.3M – 1996, Material Handling – Unit Loads and Transport Packages – Two-Dimensional symbols.

*Emerging: ISO 10303, commonly called Standard for the Exchange of Product Model Data (STEP), is a standard for the computer-interpretable representation and exchange of product data. STEP provides a neutral mechanism capable of exchanging product data between different Computer-Aided Engineering (CAE), and CAD/CAM applications. STEP supports the entire life cycle of a product, independent from any particular system, and supports 3D geometry, including 3D wireframe and 3D solid geometry.*

*Effective use of STEP to share product model data for systems requires a companion standard, ISO/IEC 13584, to exchange CAD Part Libraries (PLIB). The PLIB supplies a data model of the supplier part library, supplier identification, and part geometry.*

*MIL-PRF-28000B, a profile of IGES 5.3, is also an emerging standard for IGES. This CALS profile is based on the Y2K-compliant version of IGES and will require all IGES data files to be submitted in a Y2K-compliant format.*

## *10.1.6 Storage Media*

### 10.1.6.1 Optical Storage Media

MIL-HDBK-9660B, 1 September 1997, provides additional guidance in the use of Compact Disc-Read Only Memory (CD-ROM) technology. In cases where CD-ROM/CD-RW media is used, the following file system format (at a minimum) is mandated:

- ISO 9660:1988, Information processing – Volume and file structure of CD-ROM for information interchange.

### 10.1.6.2 Smart Cards

*Emerging: The standards for both contact and contactless Smart Cards are still evolving and being specified. The ISO 7816 series is for contact Smart Cards while ISO 10536, 14443 and 15693 specify the standards for various types of contactless smart cards.*

### 10.1.6.3 Electronic Tags

**RFID -** Radio frequency identification (RFID) is a relatively new approach to identify, categorize and locate people and materiel automatically within a few inches to 300 feet. The technology helps when a user needs to locate and redirect individual containers or needs to know the container’s contents.

In active RF tags, the labels are known as tags or transponders. They contain information that can range from a permanent ID number programmed into the tag by the manufacturer to a variable 128-kilobyte memory that can be programmed by a controller using RF energy. The controller is usually referred to as a reader or interrogator. An interrogator and a tag use RF energy to communicate with each other. The interrogator sends an RF signal that "wakes up" the tag, and

the tag transmits information to the interrogator. The interrogator also can write new information on the tag, thus permitting a user to alter the tag's information within the effective range.

There are currently no mandated standards supporting RFID.

**Satellite Tracking -** A satellite tracking system provides the ability to track the exact location of vehicles and convoys. The latitude and longitude locations of trucks, trains, and other transportation assets equipped with a transceiver are transmitted periodically via satellite to a ground station. Some systems also provide two-way communications between a vehicle operator and a ground station for safety, security and the ability to reroute.

There are currently no mandated standards supporting Satellite Tracking.

## 10.2 Facsimile

### *10.2.1 Analog Facsimile Standards*

For Facsimile (analog output) standards, which comply with the ITU-T Group 3 specifications, the following standards are mandated:

- TIA/EIA-465-A, Group 3 Facsimile Apparatus for Document Transmission, 21 March 1995.
- TIA/EIA-466-A, Procedures for Document Facsimile Transmission, 27 September 1996.

### *10.2.2 Digital Facsimile Standards*

Digital Facsimile equipment standards for Type I and/or Type II modes are used for digital facsimile terminals operating in tactical, high Bit Error Rate (BER) environments and for facsimile transmissions utilizing encryption or interoperability with NATO countries.

The following standard is mandated:

- MIL-STD 188-161D, Interoperability and Performance Standards for Digital Facsimile Equipment, 10 January 1995.

## 10.3 Electronic Data Interchange

Electronic Data Interchange (EDI) is a new Base Service Area specializing in the computer-to-computer exchange of business information using a public standard. EDI is a central part of Electronic Commerce (EC), the paperless exchange of business information. FIPS Pub161-2 establishes the Federal EDI Standards Management Coordinating Committee (FESMCC) to harmonize the development of EDI transaction sets and message standards among Federal agencies, and the adoption of Government-wide implementation conventions. The Federally approved Implementation Conventions may be viewed on the Web at: http://www.antd.nist.gov/fededi/l**.**

The DoD EDI Standards Management Committee (EDISMC) was established to coordinate EDI standardization activities within DoD. The EDISMC supports the development, adoption, publication, and configuration management of EDI implementation conventions for DoD. The

DoD EDISMC manages the efforts of several Functional Working Groups (FWGs). DoD FWGs have been established in the following areas: Logistics, Finance, Healthcare, Transportation, Procurement, and Communication, Command and Control. EDISMC-approved implementation conventions are submitted to the FESMCC for approval as Federal implementation conventions. DoD-approved implementation conventions may be viewed on the Web at: http://www-edi.itsi.disa.mil.

FIPS PUB 161-2, 22 May 1996, Electronic Data Interchange (EDI) adopts, with specific conditions, ANSI ASC X12, UN/Electronic Data Interchange for Administration, Commerce, and Transport (EDIFACT) and ANSI HL7.

The following standards are mandated as profiled by FIPS PUB 161-2:

- ANSI ASC X12 Electronic Data Interchange.
- ISO UN/EDIFACT

## 10.4 Global Positioning System

The CJCS (CJCSI 6130.01A, 1998 CJCS Master Positioning, Navigation, and Timing Plan) has declared that the GPS will be the primary radionavigation system source of positioning, navigation and timing (PNT) for DoD. GPS is a space-based, worldwide, precise positioning, velocity, and timing system. It provides an unlimited number of suitably equipped passive users with a force-enhancing, common-grid, all-weather, continuous, three-dimensional PNT capability. The NAVSTAR GPS provides two levels of service—a Standard Positioning Service (SPS) and a Precise Positioning Service (PPS).

The following standard is mandated:

- ICD-GPS-200C, NAVSTAR GPS Space Segment/Navigation User Interfaces, 16 Oct 97.

The PPS was designed primarily for U.S. military use, and DoD will control access to the PPS through cryptography. DoD GPS users with combat, combat support, or combat service support missions must acquire and use PPS-capable GPS receivers. The U.S. will enter into special arrangements with military users of allied and friendly governments to allow them use of the PPS.

The following standards are mandated:

- ICD-GPS-222A, NAVSTAR GPS UE Auxiliary Output Chip Interface (U), 26 Apr 96.
- ICD-GPS-225A, NAVSTAR GPS Selective Availability/Anti-Spoofing Host Application Equipment Design Requirements with the Precise Positioning Service Security Module (U), 12 Mar 98.

For additional information associated with the acquisition and use of PPS-capable GPS receivers, including End-of-Week Rollover compliance, and Year 2000 compliance for GPS receivers, consult the GPS JPO at the following Web site: <**http://gps.losangeles.af.mil**>.

# 11. Operating System Services

These core services are necessary to operate and administer a computer platform and to support the operation of application software. They include kernel operations, shell, and utilities. The operating system controls access to information and the underlying hardware. These services shall be accessed by applications through either the standard or WIN32 APIs.

When requiring real-time operating systems, the IEEE 1003.13:1998 Standardized Application Environment Profile – POSIX Realtime Application Support standard should be considered for use. It has been designed to satisfy a wide range of real-time system requirements based upon the Application Platform's size and function. It identifies four real-time application environment profiles based on the ISO/IEC 9945-1 series of standards including: Minimal Realtime System Profile (PSE51), Realtime Controller System Profile (PSE52), Dedicated Realtime System Profile (PSE53), and Multi-Purpose Realtime System Profile (PSE54). Not all operating-system services are required to be implemented, but those that are used shall comply with the standards listed below.

The following standards are mandated for use with POSIX-compliant operating systems running (or intended to run) POSIX-compliant applications:

- ISO/IEC 9945-series, Information Technology – Portable Operating System Interface (POSIX).
- IEEE 1003 series, IEEE Standard for Information Technology - Portable Operating System (POSIX) Open System Environment (OSE) profile.

The following standard is mandated for use with operating systems running (or intended to run) Win32 Applications:

- Win32 APIs, Window Management and Graphics Device Interface, Volume 1 Microsoft Win32 Programmers Reference Manual, 1993 or later, Microsoft Press.